PROYECTO FIN DE CARRERA

AUDITORÍA Y EVALUACIÓN DEL GRADO DE CONTROL INFORMATICO DE UNA ENTIDAD RESPECTO A LA LEY SARBANES-OXLEY

INGENIERÍA TÉCNICA EN INFORMÁTICA DE GESTIÓN

Autor: Luis Eduardo García Sánchez

Tutor: Antonio García Carmona

Leganés, 24 de Octubre de 2016

Título: Auditoría y evaluación del grado de control informático de una entidad respecto a la ley Sarbanes-Oxley

Autor: Luis Eduardo García Sánchez

Director: Antonio García Carmona

EL TRIBUNAL

Presidente: Lorena González Manzano

Vocal: Dolores Cuadra Fernández

Secretario: Alejandro Calderón Mateos

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día 24 de Octubre de 2016 en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO PRESIDENTE

Agradecimientos

En primer lugar me gustaría agradecer el esfuerzo y entendimiento a los que han sido mis dos tutores en este proyecto, empezando por Miguel Ángel Ramos que, en el trascurso del mismo llevo a cabo su jubilación y al cual le deseo lo mejor, y siguiendo con Antonio García que aunque cogió el proyecto iniciado siempre ha intentado aportarme su visión, ayuda y máximo entendimiento en una situación personal complicada. A ambos les debo su motivación y sus consejos para dar este último paso a una andadura que empecé hace algunos años.

Continuando y la verdad, más que agradecer, ya que intento hacerlo a cada momento, dedicarle esto a mis padres que siempre me han ayudado, comprendido y sabido aconsejar y guiar en mi vida, que a pesar del último año tan complicado han sabido ayudarme moralmente y hemos sido apoyo los unos para los otros y hemos hecho que al final todo haya ido a mejor y haya acabado saliendo como en este caso, mi proyecto de fin de carrera.

Y para acabar a mis amigos Jorge y Nacho que siempre han estado dispuestos a aconsejarme y aportarme sus conocimientos con una sonrisa y a Sara que siempre me ha animado y motivado a acabar lo que había empezado y, que por unos horarios tan extensos y un último año tan complicado, no terminaba de conseguirlo.

"Ni tu, ni yo, ni nadie golpea tan fuerte como la vida. Pero lo importante no son los golpes que das, si no lo que eres capaz de soportar sin bajar los brazos. Cuanto eres capaz de resistir sin tirar la toalla. Así es como se gana. Si sabes cuanto vales, exige lo que te mereces. Aguanta los golpes y no comiences a señalar ni a él, ni a ella ni a nadie porque no estas donde quieres estar. Los cobardes hacen eso y tu no eres un cobarde, tu eres mejor que eso."

Resumen

El proyecto tiene como objetivo desarrollar una metodología y, en relación a este, el diseño de un software. Este último basado en dicha metodología orientada a medir el grado confianza de los Controles Generales Informáticos en los sistemas que afectan a los estados financieros respecto a la ley Sarbanes-Oxley Act dentro de una compañía. Este se encargará de realizar preguntas correspondiendo con las distintas áreas de forma que se pueda ir evaluando cada una de ellas. Finalmente se obtendrá una conclusión final y unas recomendaciones según las respuestas aportadas.

Abstract

The project aims to develop a methodology and, in relation to this, the design of a software. The latter based on this methodology aimed at measuring the extent of IT General Controls reliance regarding the Sarbanes-Oxley Act within a company. This is responsible for conducting questions corresponding to the different areas so that they can be evaluating each of them. Finally a final conclusion and some recommendations are derived following answers provided.

ÍNDICE

GENERAL

Índice

Índice de figuras

Índice de tablas

CAPÍTULO 1

OBJETIVO Y ORGANIZACIÓN DEL PROYECTO

1. OBJETIVO Y ORGANIZACION DEL PROYECTO

Entre los principales objetivos a la hora de elegir mi proyecto de fin de carrera se encuentra la realización de un estudio técnico — teórico, que aportara un marco de referencia a las compañías a la hora de llevar a cabo una evaluación de los controles generales informáticos bajo la ley Sarbanes-Oxley; presentando adicionalmente una herramienta que permitiese evaluar de manera rápida el grado de control en los diversos sistemas con incidencia contable de la compañía.

Por esta razón el objetivo principal de este proyecto consiste en otorgar a las compañías una metodología acompañada de una herramienta práctica, sencilla e intuitiva que será la que permita evaluar los controles generales en los Sistemas de Información, en base a la anterior, que forman parte del sistema de control interno sobre el reporte financiero. Esta "auto-evaluación" estará sujeta a la ley Sarbanes-Oxley, con la que a través de ella se podrá obtener las diferentes fortalezas, deficiencias, consejos y recomendaciones necesarios para reducir el impacto de los riesgos relacionados con los sistemas financieros mediante una serie de cuestionarios que muestren su situación actual.

Conviene destacar que el objetivo que se persigue se logrará con una inversión de capital mínima o nula debido a que todas las herramientas utilizadas se encuentran distribuidas como software libre, por lo que no debe suponer ningún impedimento para las compañías que quieran apostar por este procedimiento de revisión de sus sistemas informáticos.

A continuación se especifica la distribución del Proyecto Fin de Carrera, resumiendo cada una de las partes que constituyen el mismo:

CAPÍTULO 1 - ORGANIZACIÓN DEL PROYECTO

- Comenzaré por explicar de forma general y esquemática el contenido de mi Proyecto Fin de Carrera con el fin de comprender la evolución de dicho proyecto.

CAPÍTULO 2 – ESTADO DEL ARTE

- El objetivo de este capítulo es mostrar al lector el problema de control en el ámbito informático, el impacto que ello supone y como se podría minimizar.

CAPÍTULO 3 - AUDITORÍA

- Este capítulo podría dividirse en dos secciones. La primera con un enfoque muy teórico acerca del término "auditoría" y sus tipos; y una segunda en la que se presentan los diversos organismos y estándares de referencia a la hora de evaluar y cerciorarse de que se cumplen las normas establecidas en cuanto a seguridad de la información.

CAPÍTULO 4 - LEY SARBANES-OXLEY

- En este capítulo se describen de forma general el origen, secciones, finalidades de la Ley Sarbanes-Oxley que debemos conocer a fondo acerca de la sección más utilizada en cuanto a seguridad de la información, la cual se convierte en la base de este Proyecto Fin de Carrera.

CAPÍTULO 5 – METODOLOGÍA PARA LA REVISIÓN DE CONTROLES GENERALES SOBRE SISTEMAS DE INFORMACIÓN

- En este capítulo se definirá el marco de referencia que se tendrá en cuenta a la hora de analizar la seguridad de los sistemas de información y las pautas a seguir en cuanto a la documentación de dicha evaluación.

CAPÍTULO 6 – MARCO DE EVALUACIÓN

- En este capítulo se estudiarán las diferentes preguntas/respuestas que se tendrán en cuenta para analizar la madurez del software en la aplicación a desarrollar.

CAPÍTULO 7 - APLICACIÓN PARA LA EVALUACIÓN DEL GRADO DE CONFIANZA DE LOS SISTEMAS DE INFORMACIÓN

- La finalidad de este capítulo consiste en documentar y exponer tanto las necesidades por las cuales se decide implementar este software, como las medidas y consideraciones tomadas para su desarrollo y las pruebas de su correcto funcionamiento.
- Extensa documentación de los sitios Web y referencias utilizadas para la exposición y argumentación del Proyecto de Fin de Carrera.

CAPITULO 8 – PLANIFICACIÓN Y PRESUPUESTO

- En este bloque se definen los tiempos y fechas en las que se ha llevado a cabo el proyecto así como el presupuesto detallado para llevarlo a cabo.

CAPÍTULO 9 - CONCLUSIONES

- En el último capítulo se exponen mis opiniones sobre el proyecto y el tema en general, siempre basadas en la documentación y los conocimientos adquiridos gracias a la elaboración de dicho proyecto.

CAPÍTULO 10 - LINEAS DE INVESTIGACIÓN FUTURAS

- En este capítulo se exponen diferentes líneas y temas de investigación para futuros estudiantes que crean oportuno trabajar sobre temas de controles generales en los sistemas de información.

CAPÍTULO 11 - ANEXO

GLOSARIO DE TÉRMINOS Y ACRÓNIMOS

- Diccionario técnico en el que se almacenan todos los términos y acrónimos utilizados en el documento con sus correspondientes definiciones.

BIBLIOGRAFÍA

- Documentación acerca de las referencias y sitios Web utilizados para el desarrollo y argumentación del PFC.

CAPÍTULO 2

ESTADO DEL ARTE

2. ESTADO DEL ARTE

En la actualidad, dada la complejidad que han alcanzado los procesos tecnológicos dentro de las compañías y la importancia de los sistemas de información se ha creado la necesidad de la existencia de una supervisión de los sistemas tanto por el departamento de Auditoría Interna como por Auditorías Externas.

Conviene aclarar que la Informática no gestiona propiamente la compañía, sino que ayuda a la toma de decisiones, pero no decide por sí misma. Por ello, debido a su importancia en el funcionamiento de una compañía, existe la Auditoría Informática.

Actualmente han aumentado los escándalos financieros, cosa que ha hecho caer la confianza de la opinión pública en las compañías de auditoría y contabilidad.

La auditoría ha sufrido un cambio desde la primera época en el cual el enfoque era netamente sustantivo, a uno en el cual se tiende a reducir el esfuerzo, logrando la mayor relación entre los resultados obtenidos en comparativa con el esfuerzo en horas invertido.

Esta evolución supone que se realice una validación de los Controles Generales de Sistemas de Información (ITGC) y de este modo conocer la confianza que se puede depositar en los sistemas y de este modo establecer un enfoque de auditoría con un mayor o menor grado sustantivo según las conclusiones obtenidas.

Para evitar que las compañías que cotizan en la Bolsa de Valores de Nueva York, las subsidiarias registradas en la SEC, los emisores domésticos o extranjeros que están registrados en la SEC, e incluso, hasta los proveedores de estas compañías realicen fraudes y, debido a un gran escándalo ocurrido en Estados Unidos se estableció una ley por la que todas las sociedades que deseen cotizar en dicha Bolsa deberán adaptarse a una serie de medidas.

La SOX representa un verdadero replanteamiento de la responsabilidad y la ética al interior del mundo corporativo con la intención de mejorar el ambiente de control interno de las sociedades, además de definir y formalizar responsabilidades acerca de su cumplimiento al CEO, CFO y auditores financieros.

CAPÍTULO 3

AUDITORÍA

3. AUDITORÍA

3.1 INTRODUCCIÓN

A finales del siglo XXI, los Sistemas Informáticos se han constituido en las herramientas más poderosas para materializar uno de los conceptos más vitales y necesarios para cualquier organización empresarial, los Sistemas de Información de la compañía.

La Informática hoy, está subsumida en la gestión integral de la compañía, y por eso las normas y estándares propiamente informáticos deben estar, por lo tanto, sometidos a los generales de la misma.

El concepto de auditoría es mucho más que esto. Es un examen crítico que se realiza con el fin de evaluar la eficacia y eficiencia de una sección, un organismo, una entidad, etc.

Los principales objetivos que constituyen son la base de la auditoría informática son el control de la función informática, el análisis de la eficiencia de los Sistemas Informáticos que comporta, la verificación del cumplimiento de la Normativa general de la compañía en este ámbito y la revisión de la eficaz gestión de los recursos materiales y humanos informáticos.

3.2 CONTROL INTERNO Y AUDITORÍA INFORMÁTICA

3.2.1 INTRODUCCIÓN

Históricamente en materia de control interno se adoptaba un enfoque bastante restringido limitado a los controles contables internos. Durante la última década la prensa ha informado sobre escándalos relacionados con las compañías de diferentes sectores.

Por este motivo hay cambios en las compañías correspondientes con los controles internos existentes:

1. La reestructuración de los procesos empresariales.
2. La gestión de la calidad total.
3. El redimensionamiento por reducción y/o aumento del tamaño hasta el nivel correcto.
4. La contratación externa (outsourcing).
5. La descentralización.

En general el mundo se encuentra en proceso de cambio por lo que somete a las compañías a la acción de muchas fuerzas externas tales como la creciente necesidad de acceder a los mercados mundiales, la consolidación industrial, la intensificación de la competencia y las nuevas tecnologías.

Tendencias externas que influyen en las compañías:

1. La globalización.
2. La diversificación de actividades.
3. La eliminación de ramas de negocio no rentable o antiguas.
4. La introducción de nuevos productos como respuesta a la competencia.
5. Las fusiones y la formación de alianzas estratégicas

Ante la rapidez de los cambios las sociedades deben reevaluar y reestructurar sus sistemas de controles internos para evitar fallos de control significativos. Deben tomarse medidas antes de que surjan los problemas para que de esa manera se pueda garantizar al consejo de administración, accionistas, comités y público, que los controles internos de la compañía están adecuadamente diseñados para hacer frente a los retos del futuro y asegurar la integridad en el momento actual.

El departamento de informática de una compañía suele tener una gran importancia por soportar los sistemas de información del negocio, por el volumen de recursos y presupuestos que maneja, etc. Por lo tanto aumenta las necesidades de control y auditoría, surgiendo en las organizaciones las figuras de:

CONTROL INTERNO Y AUDITORÍA INFORMÁTICA.

- La auditoría ha sufrido notables cambios a lo largo de los últimos años debido a las formas de procesar la información a partir de las distintas técnicas informáticas. Por ello la necesidad de adquirir y mantener conocimientos actualizados de los sistemas informáticos adquiere un carácter más urgente.

- Los auditores informáticos aportan conocimientos especializados, así como su familiaridad con la tecnología informática. Se siguen tratando las mismas cuestiones de control de auditoría, pero los especialistas en auditoría informática de sistemas basados en ordenadores prestan ayuda valiosa a la organización y a los otros auditores en todo lo relativo a los controles sobre dichos temas.

- En muchas organizaciones el auditor ha pasado de centrarse en la evaluación y la comprobación de resultados de procesos, desplazando su atención a la evaluación de riesgos y comprobación de controles.

- El personal de control interno informático realiza gran parte de los controles o son incorporados en programas de sistemas.

- El enfoque centrado en controles normalmente exige conocimientos informáticos a nivel de la tecnología utilizada en el área o la organización que se examina.

3.2.2 LAS FUNCIONES DE CONTROL INTERNO Y AUDITORÍA INFORMÁTICA

CONTROL INTERNO

Control Interno Informático (C.I.I.) se encarga de controlar diariamente que todas las actividades de sistemas de información sean realizadas cumpliendo los procedimientos, estándares y normas fijados por la Dirección de la Organización y/o Dirección de Informática, así como los requerimientos legales.

La misión de Control Interno es asegurarse de que las medidas que se obtienen de los mecanismos implantados por cada responsable sean correctas y válidas.

PRINCIPALES OBJETIVOS

- Controlar que todas las actividades se realicen cumpliendo los procedimientos y normas fijados, evaluar su bondad y asegurarse del cumplimiento de las normas legales.
- Asesorar sobre el conocimiento de las normas.
- Colaborar y apoyar el trabajo de Auditoría Informática, así como de las auditorías externas.
- Definir , implantar y ejecutar mecanismos y controles para comprobar el logro de los grados adecuados del servicio informático

PRINCIPALES FUNCIONES

- Realizar en los diferentes sistemas (centrales, departamentales, redes locales, etc.) y entornos informáticos (producción, desarrollo o pruebas) el control de las diferentes actividades operativas sobre:

1. Cumplimiento de diferentes procedimientos, normas y controles dictados.
2. Controles sobre la producción diaria.
3. Controles sobre la calidad y eficiencia del desarrollo y mantenimiento del software y del servicio informático.
4. Controles en las redes de comunicaciones.
5. Controles sobre el software de base.
6. Controles en los sistemas microinformáticos.
7. La seguridad informática:
   - Usuarios, responsables y perfiles de uso de archivos y bases de datos.
   - Normas de seguridad.
   - Control de información clasificada.

- Licencias.
- Contratos con terceros.
- Asesorar y transmitir cultura sobre el riesgo informático.

EL AUDITOR INFORMÁTICO (AI)

- Evalúa y comprueba en determinados momentos del tiempo, los controles y procedimientos informáticos más complejos, desarrollando y aplicando técnicas automatizadas de auditoría, incluyendo el uso de software.

- En muchos casos ya no es posible verificar manualmente los procedimientos informatizados que resumen, calculan y clasifican datos, por lo que deberá emplear software de auditoría y otras técnicas asistidas por ordenador.

- Es responsable de revisar e informar a la Dirección de la Compañía, sobre el diseño y funcionamiento de los controles implantados y sobre la fiabilidad de la información suministrada.

EL AUDITOR INFORMÁTICO (AI): FUNCIONES PRINCIPALES

Se pueden establecer tres grupos de funciones principales:

1. Participar en las revisiones durante y después del diseño, realización, implantación y explotación de aplicaciones informáticas, así como en las fases análogas de realización de cambios importantes.

2. Revisar y juzgar controles implantados en los sistemas informáticos para verificar su adecuación a las órdenes e instrucciones de la Dirección, requisitos legales, protección de confidencialidad y cobertura ante errores y fraudes.

3. Revisar y juzgar el nivel de eficacia, utilidad, fiabilidad y seguridad de los equipos e información.

3.2.3 SISTEMA DE CONTROL INFORMÁTICO: DEFINICIÓN Y TIPOS DE CONTROLES INTERNOS

Se puede definir el control interno como “cualquier actividad o acción realizada” manual y/o automáticamente para prevenir, corregir errores o irregularidades que puedan afectar al funcionamiento de un sistema para conseguir sus objetivos.

Los controles cuando se diseñen, desarrollen e implanten han de ser al menos, completos, simples, fiable, revisables, adecuados y rentables.

Los controles internos que se utilizan en el entorno informático continúan evolucionando hoy en día a medida que los sistemas informáticos se vuelven complejos.

Los progresos que se producen en la tecnología de soportes físicos y de software han modificado de manera significativa los procedimientos que se empleaban tradicionalmente para controlar los procesos de aplicaciones y para gestionar los sistemas de información.

CONTROLES INTERNOS INFORMÁTICOS: CLASIFICACIÓN

- Controles preventivos: para tratar de evitar el hecho, como un software de seguridad que impida los accesos no autorizados al sistema.

- Controles detectivos: cuando fallan los preventivos, para tratar de conocer cuanto antes el evento. Por ejemplo, el registro de intentos de acceso no autorizados, el registro de la actividad diaria para detectar errores u omisiones, etc.

- Controles correctivos: facilitan la vuelta a la normalidad cuando se han producido incidencias. Por ejemplo, la recuperación de un fichero dañado a partir de las copias de seguridad.

RELACIÓN EXISTENTE ENTRE LOS MÉTODOS DE CONTROL, LOS OBJETIVOS DE CONTROL Y LOS OBJETIVOS DE AUDITORÍA

A medida que los sistemas se han vuelto más complejos, los controles informáticos han evolucionado hasta convertirse en procesos integrados en los que se atenúan las diferencias entre las categorías tradicionales de controles informáticos.

Por ejemplo, en los actuales sistemas informáticos puede resultar difícil ver la diferencia entre seguridad de los programas, de los datos y objetivos de control del software del sistema, porque el mismo grupo de métodos de control satisface casi totalmente los tres objetivos de control.

La relación entre los métodos de control y los objetivos de control puede demostrarse en el siguiente ejemplo, en el que un mismo conjunto de métodos de control se utiliza para satisfacer objetivos de control tanto de mantenimiento como de seguridad de programas:

Objetivo de control de mantenimiento: asegurar que las modificaciones de los procedimientos programados estén adecuadamente diseñadas, probadas, aprobadas e implantadas.

Objetivo de control de seguridad de programas: garantizar que no se puedan efectuar cambios no autorizados en los procedimientos programados.

IMPLANTACIÓN DE UN SISTEMA DE CONTROL INTERNO INFORMÁTICO CRITERIO BÁSICO

- Los controles pueden implantarse a varios niveles.

- La evaluación de controles de tecnología de la Información exige analizar diversos elementos interdependientes. Por ello es importante conocer bien la configuración del sistema, para poder identificar los elementos, productos, herramientas que existen para saber dónde pueden implantarse los controles, así como para identificar los posibles riesgos.

CONOCER LA CONFIGURACIÓN DEL SISTEMA

Para llegar a conocer la configuración del sistema es necesario documentar los detalles de la red, así como los distintos niveles de control y elementos relacionados:

1. Entorno de red: esquema de la red, descripción de la configuración de hardware de comunicaciones, descripción del software que se utiliza como acceso a las telecomunicaciones, control de red, situación general de los ordenadores de entornos de base que soportan las aplicaciones críticas y consideraciones relativas a la seguridad de la red.

2. Configuración del ordenador base: configuración del soporte físico, entorno del sistema operativo, software con particiones, entornos (pruebas y real), bibliotecas de programas y conjunto de datos.

3. Entorno de aplicaciones: procesos de transacciones, sistemas de gestión de base de datos y entornos de procesos distribuidos.

4. Productos y herramientas: software para desarrollo de programas, software de gestión de bibliotecas y para operaciones automáticas.

5. Seguridad del ordenador base: identificar y verificar usuarios, control de acceso, registro e información, integridad del sistema, controles de supervisión, etc.

PARA LA IMPLANTACIÓN DE UN SISTEMA DE CONTROL INTERNO INFORMÁTICO DEBEN DEFINIRSE:

- Gestión de sistemas de información: política, pautas y normas técnicas que sirvan para el diseño y la implantación de los sistemas de información y de los controles correspondientes.

- Administración de sistemas: controles sobre la actividad de los centros de datos y otras funciones de apoyo al sistema, incluyendo la administración de las redes.

- Seguridad: incluye las tres clases de controles fundamentales implantados en el software del sistema, integridad del sistema, confidencialidad (control de acceso) y disponibilidad.

- Gestión de cambio: separación de las pruebas y la producción a nivel de software y controles de procedimientos para la migración de programas software aprobados y probados.

RESPALDO PARA LA IMPLANTACIÓN DE UNA POLÍTICA Y CULTURA DE SEGURIDAD

- Dirección de Negocio o Dirección de Sistemas de Información (S.I): Define la política y/o directrices para los sistemas de información en base a las exigencias del negocio, que podrán ser internas o externas.

- Dirección de Informática: Ha de definir las normas de funcionamiento del entorno informático y de cada una de las funciones de informática mediante la creación y publicación de procedimientos, estándares, metodología y normas, aplicables a todas las áreas de informática así como a los usuarios, que establezcan el marco de funcionamiento.

- Control Interno Informático: ha de definir los diferentes controles periódicos a realizar en cada una de las funciones informáticas, de acuerdo al nivel de riesgo de cada una de ellas, y ser diseñados conforme a los objetivos de negocio y dentro del marco legal aplicable. Estos se plasmarán en los oportunos procedimientos de control interno y podrán ser preventivos o de detección. Periódicamente realizará la revisión de controles establecidos de Control Interno Informático informando las desviaciones a la Dirección de Informática y sugiriendo cuantos cambios crea convenientes en los controles, así como trasmitirá constantemente a toda la organización de Informática la cultura y políticas de riesgo informático.

- Auditor interno/externo informático: ha de revisar los diferentes controles internos definidos en cada una de las funciones informáticas y el cumplimiento de normativa interna y externa, de acuerdo al nivel de riesgo, conforme a los objetivos definidos por la Dirección de Negocio y la Dirección de Informática. Informará a la Alta Dirección de los hechos observados y al detectarse deficiencias o ausencias de controles recomendarán acciones que minimicen los riesgos que puedan existir.
La creación de un sistema de control informático es una responsabilidad de la Gerencia y un punto destacable de la política en el entorno informático.

Figura 1. Control interno y auditoría

Figura 2. Políticas y estándares

3.3 TIPOS DE AUDITORÍA

La realización de las auditorías corresponde a los auditores, pudiéndose dividir la función auditora en dos grandes grupos: La auditoría externa y la auditoría interna. La función de auditoría informática puede existir en cualquiera de los citados entornos.

3.3.1 AUDITORÍA INTERNA

Existe en el seno de una entidad y con la iniciativa de la dirección con el ánimo de examinar y evaluar las actividades de la entidad. La responsabilidad principal del auditor interno es ayudar a la dirección en la realización de sus funciones, asegurando:

- La salvaguardia del inmovilizado material e inmaterial de la entidad.

- La exactitud y fiabilidad de los registros contables.
- El fomento de la eficiencia operativa.
- La adhesión a las políticas de la entidad y el cumplimiento de sus obligaciones legales.

El auditor interno mantiene una dedicación consistente en la adecuación de los controles sobre las actividades automatizadas, así como con la eficiencia y eficacia de los procedimientos empleados.

3.3.2 AUDITORÍA EXTERNA

Consiste en una función de evaluación independiente y externa a la entidad que se examina. En la mayoría de las compañías, se realiza una contratación anualmente con el fin de realizar una auditoría de los estados financieros, ya sea voluntariamente o por obligación legal.

3.3.3 DIFERENCIA ENTRE AUDITORÍA INTERNA Y EXTERNA

La auditoría interna se lleva a cabo con personas pertenecientes a la plantilla de la propia compañía o en algunos casos, entidades externas que colaboran con las anteriores, mientras que la externa exige, como condición esencial a la misma y de su credibilidad, que los profesionales que la realizan no formen parte de la compañía auditada, es decir que sean totalmente independientes de ella y de sus cuadros directivos.

Los trabajos de auditoría externa se desarrollan de acuerdo con normas y procedimientos internacionalmente homologados que no suelen ser substancialmente alterados ni modificados, mientras que los procedimientos de auditoría interna son mucho más flexibles y dependen, en cada caso, de la compañía, sus dirigentes y de los propios responsables de auditoría interna.

3.4 ORGANISMOS DE REFERENCIA: ISACA

Es el acrónimo de Information Systems Audit and Control Association (Asociación de Auditoría y Control de Sistemas de Información). Es una asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades auditoría y control en sistemas de información.

Ha sido la encargada de desarrollar las guías sobre Sistemas de Información emitidas hasta la fecha junto con el Instituto de Auditores Internos.

En 1967, un pequeño grupo de personas encargados de misiones similares (auditar controles en los sistemas computacionales que se estaban haciendo cada vez más críticos para las operaciones de sus respectivas organizaciones) se sentaron a discutir la necesidad de tener una fuente centralizada de información y guías en dicho campo. El grupo se formaliza

en 1969 bajo el nombre de "EDP Auditors Association" (Asociación de Auditores de Procesamiento Electrónico de Datos). Más tarde este grupo formaría una fundación de educación para llevar a cabo proyectos de investigación de gran escala para expandir los conocimientos y el valor en el campo de gobierno y control de TI.

Hoy en día los miembros de ISACA se caracterizan por su diversidad. Algunos son nuevos en el campo, otros están en niveles medios de la gerencia y algunos otros están en los rangos más elevados, cubriendo una gran variedad de puestos (consultores, auditores, profesionales de seguridad,...). Trabajan en casi todas las categorías de industrias, incluyendo finanzas y banca, firmas de auditoría y consultoría, gobierno y sector y servicios públicos. Esta diversidad permite el aprendizaje mutuo, e intercambien puntos de vista comunes sobre una variedad de tópicos profesionales. Esta ha sido considerada durante mucho tiempo como una de las fortalezas de ISACA. Previamente conocida como la Asociación de Auditoría y Control de Sistemas de la Información, ISACA ahora identificada ya por su acrónimo, para reflejar el amplio rango de profesionales del gobierno de las TI a los que sirve.

Desde su creación, ISACA se ha convertido en una organización global que establece las pautas para los profesionales del gobierno, control, seguridad y auditoría de información. Sus normas de auditoría y control son seguidas por profesionales de todo el mundo y sus investigaciones abordan temas profesionales que son desafíos para sus constituyentes.

Otra de las fortalezas de ISACA es su red de capítulos. ISACA tiene una gran extensión de capítulos en más de 80 países de todo el mundo, y dichos capítulos brindan a los miembros educación, recursos compartidos, asesoría, red de contactos profesionales y una amplia gama de beneficios adicionales a nivel local.

ISACA además ofrece cuatro certificaciones:

- La principal: Certified Information Systems Auditor (Auditor Certificado de Sistemas de Información) más conocida por su acrónimo CISA. Reconocida de forma global.
- La certificación CISM: Certified Information Security Manager (Gerente Certificado de Seguridad de Información), se concentra exclusivamente en el sector de gerencia de seguridad de la información.
- La certificación Certified in the Governance of Enterprise IT (Certificado en Gobierno de TI de la Compañía) con acrónimo CGEIT; promueve el avance de profesionales que desean ser reconocidos por su experiencia y conocimiento relacionados con el Gobierno de las TI.
- CRISC, La nueva certificación Certified in Risk and Information Systems Control (Certificado en Riesgos y Controles de los Sistemas de Información) es para profesionales de TI que identifican y gestionan los riesgos a través del desarrollo, implementación y mantenimiento de controles de SI.

ISACA publica una revista técnica líder en el campo de control de la información el "ISACA Journal". Organiza conferencias internacionales que se concentran en tópicos técnicos pertinentes a las profesiones de aseguramiento, control, seguridad y gobierno de las TI y de SI. Juntos, ISACA y su afiliado IT Governance Institute "Instituto de Gobierno de TI" (ITGI) lideran la comunidad de control de tecnología de la información y sirven a sus asociados brindando los elementos que necesitan los profesionales de TI en un entorno mundial en cambio permanente.

CAPÍTULO 4

LEY SARBANES-OXLEY

4. LEY SARBANES-OXLEY

4.1 NACIMIENTO DE SARBANES-OXLEY (SOX)

La ley SOX (Sarbanes-Oxley) nació como respuesta a una serie de escándalos corporativos que afectaron a compañías estadounidenses a finales del 2001, producto de quiebras, fraudes y otros manejos administrativos no apropiados, que mermaron la confianza de los inversores respecto de la información financiera emitida por las compañías.

Así, en julio de 2002, el gobierno de Estados Unidos aprobó la ley Sarbanes-Oxley, como mecanismo para endurecer los controles de las compañías y devolver la confianza perdida. El texto legal abarca temas como el buen gobierno corporativo, la responsabilidad de los administradores, la transparencia, y otras importantes limitaciones al trabajo de los auditores.

4.2 COMPAÑÍAS A LAS QUE APLICA

Esta ley estadounidense es aplicable a todas las compañías que están registradas en la New York Stock Exchange (NYSE) y la National Association of Securities Dealers by Automatic Quotation, conocida como NASDAQ, y bajo la supervisión de la Securities and Exchange Commission (SEC). Por lo tanto, también rige para todas las compañías extranjeras que cotizan en dichas bolsas de valores, incluyendo a la casa matriz, las subsidiarias y afiliadas.

4.3 QUÉ REGULA

La SOX contiene 11 títulos y numerosas secciones, regulando diferentes aspectos e involucrando a los ejecutivos de las compañías, directorio, gobiernos corporativos, comités de auditoría y firmas auditoras, entre otros.

Lo primero que hace la ley, es crear el "Public Company Accounting Oversight Board", más conocido como PCAOB, que es la Junta de Supervisión de Firmas de Contabilidad Pública y que comenzó a operar en abril de 2003. Su principal función es llevar el registro de las firmas auditoras, inspeccionar su trabajo y verificar que cumplan con los estándares de control de calidad y principios éticos. El PCAOB puede aplicar sanciones y medidas disciplinarias.

4.4 SECCIÓN 404

Esta sección promueve los mecanismos de supervisión y control, otorgando confianza y transparencia en la información financiera.

Las normas propuestas en la Sección 404 son aplicables a los ejercicios terminados a partir del 15 de abril de 2005, inclusive.

Esta sección establece que:

- La dirección tiene la responsabilidad sobre el establecimiento, mantenimiento y operatividad de una estructura y unos procedimientos de control interno adecuados para el reporte financiero.
- Identifique el marco sobre el que opera la Dirección para determinar la evaluación de la efectividad de los controles de la compañía sobre reporte financiero.
- La alta gerencia de las compañías sujetas a los requerimientos de la sección 404 (CEO y CFO) está obligada a incluir en sus informes anuales una evaluación de la efectividad con que funcionan los controles internos sobre la información financiera.

Si una deficiencia significativa es identificada a la fecha de los estados financieros, debe ser revelada en el informe de la gerencia. La definición de deficiencia significativa que realiza el pronunciamiento número 2 del PCAOB establece un umbral muy pequeño para categorizarlas, y por lo tanto muchas de estas pueden constituir debilidades materiales.

Por otro lado, exige al auditor externo que:

- Emita un informe validando las declaraciones efectuadas por la dirección.

Se muestra un Modelo de Control Interno sobre el reporte financiero para el cumplimiento de los requisitos recogidos en la Sección 404 de la ley Sarbanes-Oxley (SOX). El modelo mencionado recoge los siguientes tres niveles de control:

- Los controles generales: son aquellos establecidos directamente por la Dirección de la Sociedad.
- Los controles específicos (nivel proceso): son aquellos que afectan de forma individual a cada proceso al objeto de minimizar el impacto de los riesgos financieros presentes en el mismo.
- La evaluación del Control Interno es la supervisión (y valoración) del funcionamiento de los controles específicos y generales realizada por personal independiente de aquel encargado de la planificación, diseño, implantación y realización de los mecanismos de control y de las actividades propias de los procesos, que también hace o debe hacer su propia supervisión.

El siguiente gráfico es una representación del Modelo ICFR (Control Interno sobre el Reporte Financiero) mencionado anteriormente.

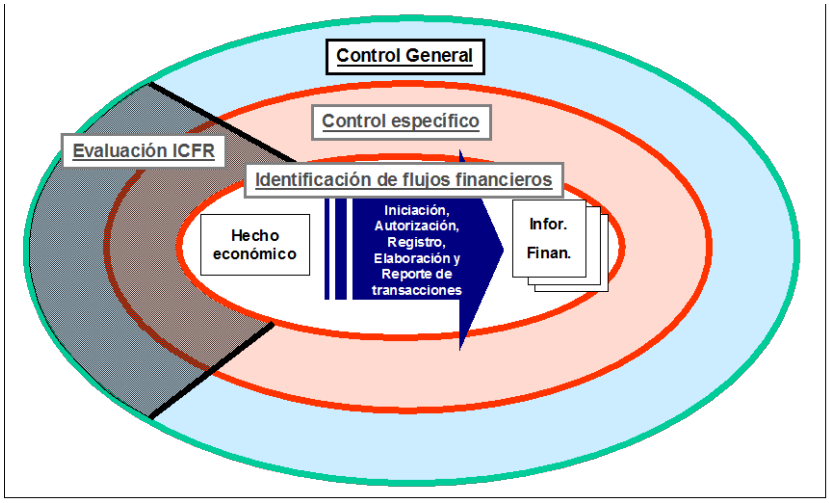


Figura 3. Modelo ICFR

Los Sistemas de Información basados en tecnología (IT) son elementos a considerar dentro del alcance de la evaluación del Control Interno sobre el reporte financiero, siempre y cuando den soporte a procesos con impacto en la información financiera. Por tanto, en sí mismos no tienen una relevancia significativa.

Según establece el Auditing Standard Nº 2 del Public Company Accounting Oversight Board (PCAOB) a continuación:

"Some controls (such as company-level controls, described in paragraph 53) might have a pervasive effect on the achievement of many overall objectives of the control criteria. For example, information technology general controls over program development, program changes, computer operations, and access to programs and data help ensure that specific controls over the processing of transactions are operating effectively. In contrast, other controls are designed to achieve specific objectives of the control criteria. For example, management generally establishes specific controls, such as accounting for all shipping documents, to ensure that all valid sales are recorded".

Además de los controles generales sobre Sistemas, expresamente recogidos en el Auditing Standard Nº 2 como controles a incluir en el alcance de la evaluación, existen algunos objetivos de control específicos relativos a los Sistemas de Información que forman parte del Modelo General de Evaluación.

4.5 IMPACTO EN IT

El área de IT es la fuente de riesgos que impacta sobre el control interno de los informes financieros, en temas tales como:

- Confiabilidad en sistemas o programas que procesan inadecuadamente datos, o procesan datos inadecuados
- Cambios no autorizados en datos, transacciones, archivos maestros y aplicaciones
- Inadecuados cambios de emergencia en aplicaciones
- Intervención manual inapropiada
- Potencial pérdida de datos

4.6 ALCANCE DE LA EVALUACIÓN DE LOS CONTROLES GENERALES SOBRE SISTEMAS DE INFORMACIÓN

El objetivo de los Controles Generales sobre Sistemas de Información es alcanzar un grado de control interno mínimo en el desarrollo, explotación y operación de todos los sistemas implantados en la Sociedad.

Para realizar la evaluación sobre la eficacia de los Controles Generales de los sistemas de información, únicamente se considerarán aquellos sistemas con impacto significativo en la información financiera en la medida que soporten parte de los procesos de reporte financiero.

Con carácter general se han considerado los siguientes tipos de Sistemas de Información:

- ERPs[1]
- Sistemas de Facturación
- Sistemas de RR.HH. (Nóminas)
- Sistemas de consumo (Sistema de registro de tráfico, ...)

4.7 METODOLOGÍAS DE EVALUACIÓN

De acuerdo al Sarbanes Oxley Act, las organizaciones deben seleccionar e implementar un marco de referencia para el control interno.

PCAOB (Public Company Accounting Oversight Board) propone COSO como el marco de referencia a utilizar para realizar la evaluación. También existen otras referencias de metodología aplicables en materia de Auditoría de Sistemas de Información que han sido consideradas en el desarrollo de la metodología de evaluación de controles generales sobre Sistemas de Información. Algunas de las más importantes para los profesionales de la contabilidad y la auditoría son:

[1] La categoría de ERPs incluye los sistemas contables propiamente dichos como por ejemplo SAP y otros sistemas cuyo objetivo principal puede no ser el registro de información financiera, aunque recogen información básica que soporta saldos contables registrados (Ejemplo: Sistemas de logística, Sistema de gestión de activos, ...)

4.7.1 C.O.S.O

4.7.1.1 DEFINICIÓN DE C.O.S.O

El Comité de Organizaciones Patrocinadoras de la Comisión Treadway, en inglés, Committee of Sponsoring Organizations of the Treadway Commission (C.O.S.O.) es una organización voluntaria del sector privado, establecida en los Estados Unidos y dedicada a orientar en el ámbito privado y gubernamental sobre aspectos relevantes de gestión de la organización, control interno de la compañía, gestión del riesgo, el fraude y la presentación de informes financieros. El "Informe C.O.S.O." es un documento que describe un modelo común de control interno con el que las organizaciones pueden implantar, gestionar y evaluar sus sistemas de control interno para garantizar que estos se mantengan funcionales, eficaces y eficientes.

4.7.1.2 MOTIVOS PARA EL DESARROLLO DEL INFORME C.O.S.O

A medida que el tiempo iba trascurriendo, las organizaciones fueron implementando sus propias políticas para el desarrollo del control interno, ocasionando una gran variedad de conceptos a la vez que disconformidades en la práctica de control interno. Teniendo en cuenta esta situación era necesario estandarizar unas mejores prácticas con respecto al control interno. La posibilidad de contar con un marco facilitaría la comprensión y desarrollo de nuevos métodos de control interno que se adapten a la realidad actual y brinden una referencia conceptual común sobre éste.

- Definir un concepto común de control interno que especifique las mejores prácticas en el mismo.
- Depositar un modelo con el fin de que las entidades puedan evaluar su nivel de control interno.
- Fomentar la idea de que el control interno sea una práctica habitual en las organizaciones.
- Disponer de una guía común tanto para auditores como para auditados, de tal manera que todos manejen el mismo marco conceptual.

4.7.1.3 MARCO INTEGRADO DE CONTROL

A la hora de enfocar un control sobre un sistema integrado una de las pautas fundamentales es cubrir los cinco componentes de TI que se encuentran integrados en los procesos administrativos. Dichos componentes responden dinámicamente a las condiciones y formas que tiene la Compañía de manejar su "core" del negocio, donde algunos de ellos forman parte de un proceso multidireccional que puede influir en uno o varios de los otros componentes.

A continuación se detallan los cinco componentes anteriormente comentados.

AMBIENTE DE CONTROL

Cuando se habla del ambiente de control que rodea a la revisión de una compañía se refiere al conjunto de hechos o casuísticas que determinan la forma de actuar de una entidad desde la perspectiva del control interno, es decir, los procedimientos y metodologías que deben aplicar de manera interna dependen de las características que rodeen al tipo de negocio sobre el que se quiere realizar dicho control.

El ambiente de control permite fijar una base sólida que permite imponer disciplina de trabajo sobre su personal, de ahí su gran importancia, pues la correcta adecuación de las políticas y procedimientos al ambiente individual de la entidad permitirá obtener resultados efectivos y eficientes a la organización.

Algunos de los principales factores que se tienen en cuenta a la hora de evaluar el ambiente de control son:

- La estructura y plan organizacional de la entidad.
- La filosofía, competencia profesional y compromiso de todos los niveles, así como su correcta adhesión a las políticas preestablecidas.
- Los métodos de asignación de responsabilidades.
- El grado de documentación de políticas y procedimientos.
- La existencia, o no, de comités de auditoría; analizando la cualificación y el grado de independencia de las personas que lo forman.

El ambiente de control será dispar e independiente para cada entidad por lo que su correcto o incorrecto grado de adecuación se verá reflejado en las fortalezas o debilidades que se generen en las distintas áreas de la organización.

EVALUACIÓN DE LOS RIESGOS

Si hubiera que definir la función más importante del control interno sin lugar a dudas sería la de limitar los riesgos concernientes a las actividades que afectan al negocio de las organizaciones. Es por ello que para poder combatir los riesgos que puedan incidir negativamente el primer paso consiste en adquirir un conocimiento práctico y global de todos los componentes de los que consta el negocio con el fin de poder neutralizar las vulnerabilidades de los mismos, tanto a nivel interno como externo.

Previa identificación de riesgos es necesario establecer unos objetivos base sobre los que investigar y analizar sus posibles debilidades; los objetivos pueden ser tanto explícitos como implícitos, pero siempre deben de englobar tanto aspectos genéricos

como específicos de cada actividad crítica. No menos importante es la correcta definición de los criterios que permitirán evaluar el rendimiento de los objetivos pues una buena definición permitirá catalogar los objetivos como adecuados, completos, razonables o integrables en el cómputo global de la organización.

A la hora de analizar los riesgos de una entidad se debe cubrir tres fases:

- Estimación de la relevancia del riesgo.
- Evaluación de la probabilidad de ocurrencia del mismo.
- Determinación del plan de acción ante el acontecimiento de uno de ellos.

El mundo de las tecnologías de la información se encuentra en un constante proceso de cambio en el cual se necesitan mecanismos cada vez más sofisticados que permitan encarar con un grado de confianza relevante los riesgos asociados con el cambio; es por ello que la gestión de los cambios merece efectuarse de manera independiente al resto de riesgos dada su gran importancia en los aspectos referentes a:

- Cambios de entorno
- Políticas institucionales
- Reestructuraciones internas
- Gestión de empleados
- Nuevas normativas y tecnologías

ACTIVIDADES DE CONTROL

Ya que las actividades de control abordan todos los niveles de cada etapa de la gestión del negocio siempre podremos encuadrar los controles dependiendo del objetivo que queramos cubrir: operaciones, confiabilidad de los datos financieros o cumplimiento normativo y legal; siempre eligiendo el mejor tipo de control disponible (preventivo/ correctivo, manual/ automático, gerencial/ directivo, etc.).

Es necesario remarcar la importancia de contar con buenos controles de TI, pues éstos desempeñan un papel clave en la gestión, el procesamiento de datos, la implantación y mantenimiento del software, la seguridad en el acceso a los sistemas, los proyectos de desarrollo y mantenimiento de las aplicaciones. Siempre necesitando de una respuesta por parte de un personal cualificado. Pero tan importante es tener un personal cualificado como que la información relevante sea procesada y transmitida de manera eficiente puesto que de ello depende la correcta dirección y control de las operaciones.

INFORMACIÓN Y COMUNICACIÓN

La comunicación es inherente a los sistemas de información, por lo que cada función debe especificarse con claridad entendiendo las responsabilidades que se le asignan a cada persona dentro del sistema de control interno. Además de una buena comunicación interna, mantener una comunicación externa eficaz favorece el flujo de toda la información necesaria; para ello se puede hacer uso de diferentes elementos, dentro de los cuales se encuentran manuales de políticas, memorias, difusión institucional, etc. Una compañía con una historia basada en la integridad y una sólida cultura de control no tendrá dificultades de comunicación.

Como bien sabemos, los sistemas de información permiten identificar, recoger, procesar y divulgar datos relativos a las actividades internas y externas, y funcionan muchas veces como herramientas de supervisión a través de rutinas previstas para tal efecto. No obstante es de relativa importancia mantener actividades estratégicas a través de la evolución de sistemas exclusivamente financieros a otros integrados con las operaciones para un mejor seguimiento y control de las mismas; así como concluir la revisión con la transferencia adecuada del informe de seguimiento y resultados que arroja el control realizado.

SUPERVISIÓN

Una de las labores primordiales de la Dirección de una compañía consiste en establecer una estructura eficiente y organizada de control interno la cual incluya una revisión periódica de sus niveles de calidad preestablecidos y definidos que permita evaluar sus niveles de cumplimiento de forma temporal, tanto para las áreas que mayor desarrollo poseen como aquellas que por su pérdida de eficacia es necesario su reemplazo o cambio de visión. El ámbito al que se refieren dichos cambios puede ser tanto cambios de nivel interno como externo y pueden generar nuevos riesgos que la Dirección debe de poder soportar.

Para llevar a cabo esta revisión del control interno se pueden utilizar dos enfoques igualmente válidos que pueden ser aplicados de manera individual o combinada: las actividades continuas (aquellas que hacen uso de actividades de gestión recurrentes y repetitivas, siempre ejecutadas en tiempo real con el fin de evaluar las respuestas del usuario en las circunstancias concretas) y las evaluaciones puntuales. Dentro de las evaluaciones puntuales al ser pruebas que pueden ser muy diferentes entre sí, es importante tener en cuenta los siguientes aspectos:

a) El plan de acción para evaluar el control debe contener siempre los siguientes puntos:

- Alcance de la evaluación.
- Listado de actividades continuadas de supervisión existentes.
- Definición de las funciones de los auditores internos y externos.
- Evaluación de los riesgos de cada área a auditar.
- Documentación relativa al marco de metodologías y herramientas a utilizar.
- Conclusiones y recomendaciones.
- Acciones de seguimiento preestablecidas tras la aplicación de las recomendaciones.

b) A la hora de definir tanto la frecuencia como el alcance de la evaluación pueden afectar factores como: el riesgo que puede conllevar realizarla en un momento concreto, la naturaleza del cambio o la competencia y experiencia del personal encargado de llevarla a cabo.
c) El principal objetivo del evaluador debe fundamentarse en conocer el funcionamiento del sistema que se está analizando, englobando todos los enfoques y técnicas utilizados y revisando que todos los controles se encuentren formalizados y se ejecuten de manera rutinaria en el día a día de la Compañía.
d) Deben de ser ejecutadas por los responsables de las áreas de gestión y auditoría interna así como por auditores externos con el fin de cubrir la objetividad y rigurosidad deseada.
e) Se deben de utilizar metodologías concretas y testadas con anterioridad que permitan evaluar la eficacia de forma correcta.
f) La documentación de los procedimientos debe ser un punto importante dentro de la organización. Esto no es únicamente relevante a la hora de tener que demostrar la fortaleza del sistema ante terceros, sino que un nivel adecuado de documentación procedimental permite y facilita la comprensión de los controles por parte de los usuarios de una manera eficiente y rigurosa.

Una vez cerrada la evaluación se debe preparar un escrito documentado y lo más específico posible en el que se muestren tanto los puntos de mejora y debilidades del sistema inspeccionado como las correspondientes recomendaciones que el auditor establece como necesarias para que la organización se ajuste a las normativas vigentes y estipuladas. Dicho informe debe ser comunicado tanto al personal responsable de la Compañía en lo concerniente a TI como a las autoridades pertinentes en el supuesto de que se esté incurriendo en un incumplimiento grave de normativas sancionables.

4.7.2 COBIT

El Informe COBIT (emitido por el IT Governance Institute) fue elaborado como un estándar generalmente aplicado y aceptado sobre las políticas de seguridad y los controles sobre Sistemas de Información, proporcionando un marco de referencia para su desarrollo.

Basado en el Informe COSO y mostrando los objetivos de control:

- la efectividad y la eficiencia de las operaciones
- la confidencialidad e integridad de la información financiera
- el cumplimiento de las leyes y regulaciones en materia de Auditoría de Sistemas de Información.

Muestra la filosofía de que los Sistemas de Información son administrados a través de un número limitado de procesos.

La evaluación de los requerimientos del negocio, los recursos y procesos IT, son aspectos importantes para el correcto funcionamiento de una compañía, lo que conlleva la supervivencia en el mercado.

Consiste en un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores IT, usuarios y además, los auditores involucrados en el proceso.

COBIT es un modelo de evaluación y monitorización centrado en el control de negocios y la seguridad IT y que abarca controles específicos de IT desde una perspectiva del negocio.

Las siglas COBIT significan Objetivos de Control para Tecnología de Información y Tecnologías relacionadas (Control Objectives for Information Systems and related Technology). El modelo es el resultado de una investigación con expertos de varios países, desarrollado por ISACA (Information Systems Audit and Control Association).

COBIT, lanzado en 1996, es una herramienta de gobierno de TI que ha cambiado la forma en que trabajan los profesionales de tecnología. Relacionando tecnología informática y prácticas de control. En este modelo se consolidan los estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores.

COBIT se aplica a los sistemas de información de toda la compañía, incluyendo los equipos personales y las redes. Está basado en la filosofía de que los recursos TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

La estructura del modelo COBIT propone un marco de acción donde se evalúan los criterios de información, como por ejemplo la seguridad y calidad, se auditan los recursos que comprenden la tecnología de información, como por ejemplo el recurso humano, instalaciones, sistemas, entre otros, y finalmente se realiza una evaluación sobre los procesos involucrados en la organización.

La adecuada implementación de un modelo COBIT en una organización, provee una herramienta automatizada, para evaluar de manera ágil y consistente el cumplimiento de los objetivos de control y controles detallados, que aseguran que los procesos y recursos de información y tecnología contribuyen al logro de los objetivos del negocio en un mercado cada vez más exigente, complejo y diversificado.

A partir de los 32 procesos en los que se subdivide la administración de los Sistemas de Información se definen 32 objetivos de control generales, uno para cada uno de los procesos. A continuación se presenta la relación de dominios mencionados por COBIT y los procesos relacionados con cada uno de los dominios:

- Dominio: Planificación y organización

  Po1 Definición de un plan estratégico
  Po2 Definición de la arquitectura de información
  Po3 Determinación de la dirección tecnológica
  Po4 Definición de organización y relaciones
  Po5 Administración de la inversión
  Po6 Comunicación de las políticas
  Po7 Administración de los recursos humanos
  Po8 Asegurar el cumplimiento con los requerimientos Externos
  Po9 Evaluación de riesgos
  Po10 Administración de proyectos
  Po11 Administración de la calidad
- Dominio: Adquisición e implementación

  A11. Identificación de soluciones automatizadas
  A12. Adquisición y mantenimiento del software aplicativo
  A13. Adquisición y mantenimiento de la infraestructura tecnológica
  A14. Desarrollo y mantenimiento de procedimientos
  A15. Instalación y aceptación de los sistemas
  A16. Administración de los cambios
- Dominio: Prestación y soporte

  Ds1. Definición de los niveles de servicios
  Ds2. Administrar los servicios de terceros
  Ds3. Administrar la capacidad y rendimientos
  Ds4. Asegurar el servicio continuo
  Ds5. Asegurar la seguridad de los sistemas
  Ds6. Entrenamiento a los usuarios

Ds7. Identificar y asignar los costos

Ds8. Asistencia y soporte a los clientes

Ds9. Administración de la configuración

Ds10. Administración de los problemas

Ds11. Administración de los datos

Ds12. Administración de las instalaciones

Ds13. Administración de la operación

- Dominio: Control

M1. Monitorización del cumplimiento de los objetivos de los procesos de tecnología de la información.

M2. Obtener realización de las evaluaciones independientes

Actualmente COBIT se encuentra en la versión 5 (lo mencionado anteriormente correspondía a la 4.1).

En la fecha 10 de abril de 2012, ISACA realizo de forma oficial una publicación de la nueva versión de COBIT 5, la cual incluye cambios relativos a cantidad y distribución de procesos respecto al borrador que se emitió en junio 2011.

En consecuencia, se refleja a continuación como quedaría la actualización del diagrama de procesos:

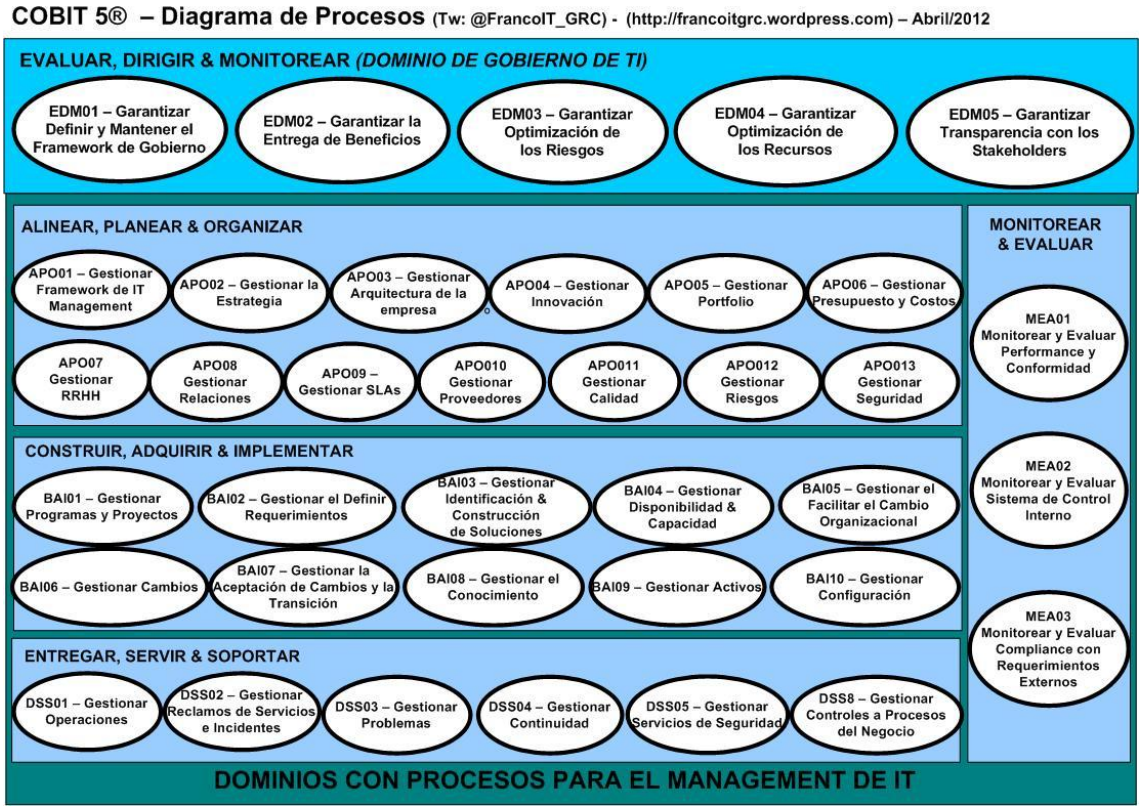


Figura 4. Dominios con procesos para el management de IT

En el siguiente mapa se realiza un análisis del marco de trabajo de COBIT 5:

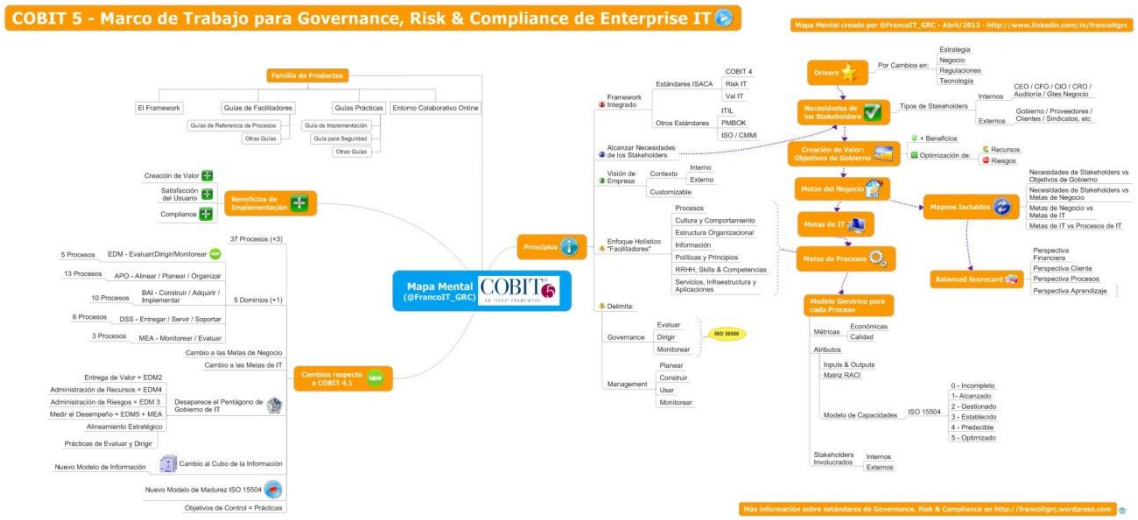


Figura 5. Marco de trabajo COBIT 5

Como se puede apreciar, existen unas relaciones complejas entre los distintos elementos que componen COBIT 5, la cual incluye los siguientes aspectos:

Procesos y Dominios:

A nivel de la estructura de Procesos y Dominios se comprueba lo siguiente:

- Existe un nuevo Dominio (ahora son 5), que se enfoca en aspectos de Gobierno de TI, denominado "EDM – Evaluar, Dirigir & Monitorear" y que cubre el antiguo proceso ME4 de COBIT 4.
- El número de procesos se ha incrementado de 34 a 37.
- Se han modificado los dominios para algunos objetivos de control:
  - PO10 – Administrar los proyectos, pasó al Dominio BAI.
  - AI5 – Procurar recursos de IT, pasó al Dominio APO.
  - DS1 – Definir y Administrar los niveles de servicio, pasó al Dominio APO.
  - DS2 – Administrar los servicios de Terceros, pasó al Dominio APO.
  - DS3 – Administrar el desempeño y la capacidad, pasó al Dominio BAI.
  - DS6 – Identificar y asignar costos, pasó al Dominio APO.
  - DS7 – Educar y Entrenar a los usuarios, pasó al Dominio APO.
- En el dominio APO – Administrar, Planear y Organizar, es donde se observa mayor reorganización interna de los objetivos de control, es decir que un antiguo proceso de COBIT 4, ahora puede estar distribuido como parte de hasta 5 procesos del mismo dominio en COBIT 5.
- El proceso DS12 – Administrar el Ambiente Físico ahora forma parte del DSS5.
  - Gestionar los Servicios de Seguridad
- Existen nuevos procesos cuyo contenido es mayormente producto de COBIT 5, destacándose:

- EDM1 – Definir el Framework para el Governance
- APO1 – Definir el Framework para el Management
- APO4 – Gestionar Innovación
- APO13 – Gestionar Seguridad (también hay un Proceso DSS05 Gestionar los Servicios de Seguridad)
- BAI8 – Gestión del Conocimiento

A continuación, se indica un cuadro con la relación entre los procesos de COBIT 4.1 y su cobertura en COBIT5, manteniendo como fuente de la información el material de ISACA incluido en Anexo de la Guía de Procesos de Referencia, pero dado que estaba desglosado por Objetivo de Control, se agrupo a nivel Proceso, destacando como "Primaria" al Proceso de COBIT 5 que mayor porcentaje de cobertura les otorga a los objetivos de control del antiguo proceso de COBIT 4.1.

COBIT 4.1		COBIT 5 - Cobertura (P)rimaria y (S)ecundaria	
Proceso	Descripción	Primaria	Secundaria
PO	Planear y Organizar	Alinear, Planear y Organizar	
PO1	Definir un plan estratégico de TI	APO02	EDM02 / APO05
PO2	Definir la arquitectura de la información	APO03	APO01
PO3	Definir la dirección tecnológica	APO02 / APO04	EDM01 / APO03 / APO01
PO4	Definir los procesos organización y relaciones de TI	APO01	APO07 / APO11 / DSS06
PO5	Administrar la inversión en TI	APO06	APO05
PO6	Comunicar las metas y la dirección de la gerencia	APO01	EDM03
PO7	Administrar los recursos humanos de TI	APO07	APO01
PO8	Administrar la calidad	APO11	
PO9	Evaluar y administrar los riesgos de TI	APO12	EDM03 / APO01
PO10	Administrar los proyectos	BAI01	
AI	Adquirir e Implementar	Construir, Adquirir e Implementar	
AI1	Identificar las soluciones automatizadas	BAI02	
AI2	Adquirir y mantener software aplicativo	BAI03	
AI3	Adquirir y mantener la infraestructura tecnológica	BAI03	DSS02
AI4	Facilitar la operación y el uso	BAI08	BAI05
AI5	Procurar recursos de TI	APO10	BAI03
AI6	Administrar los cambios	BAI06	
AI7	Instalar y acreditar las soluciones y cambios	BAI07	BAI05
DS	Entregar Servicio	Entregar Servicio y Soportar	
DS1	Definir y administrar los niveles de servicio	APO09	
DS2	Administrar los servicios de terceros	APO10	
DS3	Administrar el desempeño y la capacidad	BAI04	
DS4	Asegurar el servicio continuo	DSS04	
DS5	Garantizar la seguridad de los sistemas	DSS05	APO13
DS6	Identificar y asignar costos	APO06	
DS7	Educar y entrenar a los usuarios	APO07	
DS8	Administrar la mesa de servicio y los incidentes	DSS02	
DS9	Administrar la configuración	BAI10	DSS02
DS10	Administrar los problemas	DSS03	
DS11	Administrar los datos	DSS04	DSS01 / DSS05 / DSS06
DS12	Administrar el ambiente físico	DSS01 / DSS05	
DS13	Administrar las operaciones	DSS01	DSS05 / BAI09
ME	Monitorear y Evaluar	Monitorear y Evaluar	
ME1	Monitorear y evaluar el desempeño de TI	MEA01	
ME2	Monitorear y evaluar el control interno	MEA02	
ME3	Garantizar el cumplimiento regulatorio	MEA03	
ME4	Proporcionar gobierno de TI	EDM01 / EDM02 / EDM03 / EDM04 / MEA02	

Tabla 1. Objetivos de proceso COBIT 4.1

Metas de Negocio y Metas de TI:

- Respecto a la relación habitual entre Metas de Negocio y Metas de TI, COBIT 5 ha llevado a cabo una mejora en relación a la precisión del grado de relevancia de dicho nexo, dado que se divide en “Primaria” o “Secundaria.

Figura 6. Metas de negocio y metas de IT

- En COBIT 5 se mantiene la cantidad de Metas de Negocio (17) pero ha sufrido modificaciones relativas a sus contenidos y la distribución tal como se detalla a continuación:

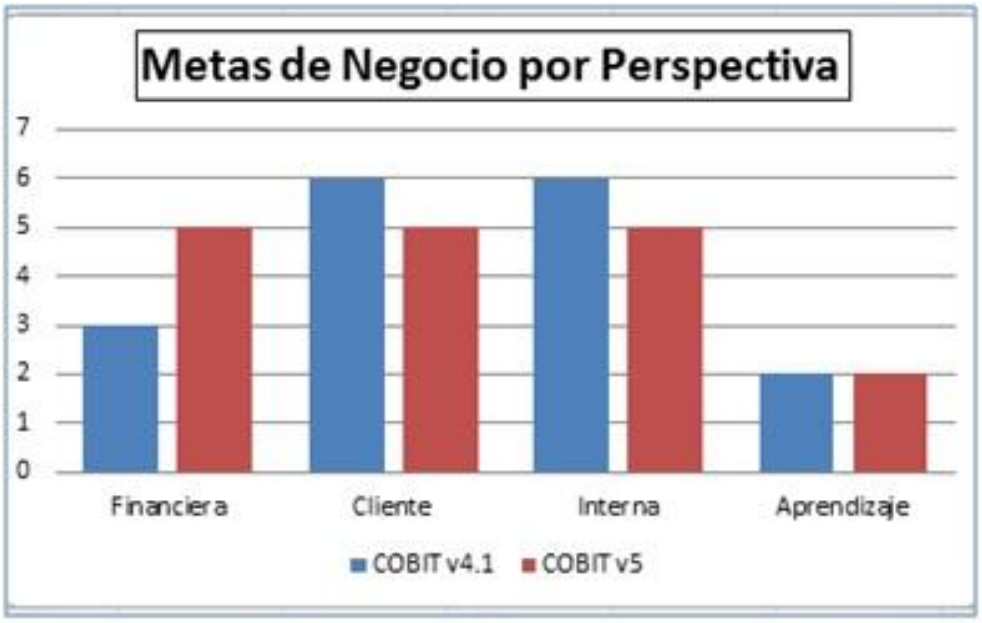


Figura 7. Metas de negocio por perspectiva

Se han realizado dos cambios de relevancia respecto a las Metas de TI:

- Disminuyó la cantidad de 28 a 17 Metas.
- Para cada Meta de TI se indica la relación con la Perspectiva del Balanced Scorecard:

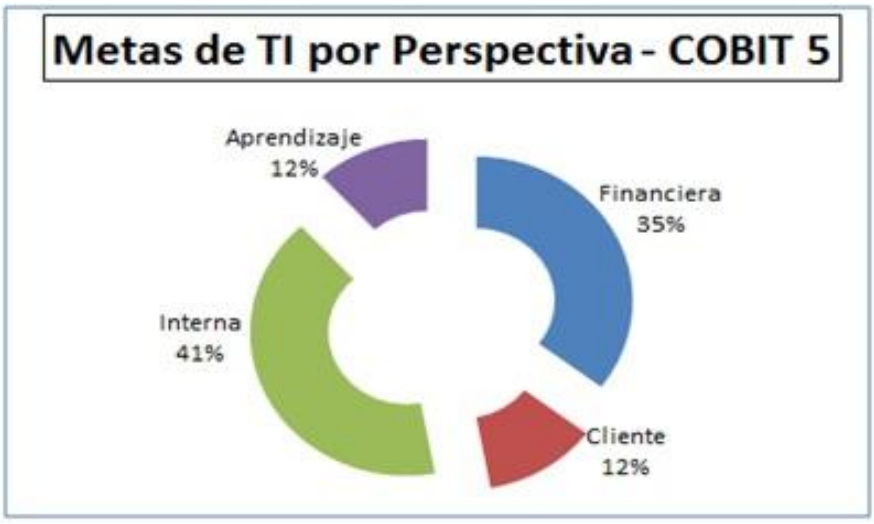
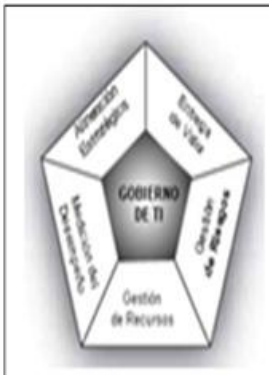


Figura 8. Metas de IT por perspectiva COBIT 5

El Pentágono de COBIT 4.1 para el Gobierno de TI:

Se ha creado un nuevo dominio a partir del "Pentágono" del Gobierno TI denominado "EDM – Evaluar / Dirigir & Monitorear":

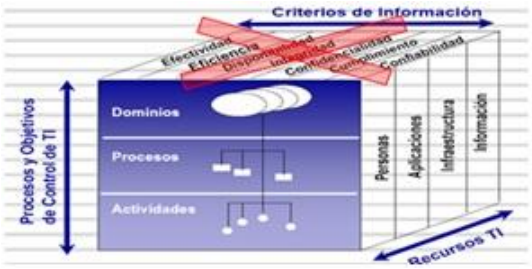


Pentágono de COBIT 4.1:	Cobertura en COBIT 5:
Alineación Estratégica	Prácticas de Evaluar y Dirigir (Governance) Práctica de Dirigir (Management)
Entrega de Valor	Proceso EDM2
Gestión de Riesgos	Proceso EDM3
Gestión de Recursos	Proceso EDM4
Medición del Desempeño	Proceso EDM5 y Práctica de Monitoreo

Figura 9. Pentágono de COBIT 4.1 y cobertura en COBIT 5

El Cubo de COBIT 4.1 para los Criterios de la Información:

Se ha implantado un nuevo Modelo de la Información que sustituirá a los 7 Criterios que en la anterior versión de COBIT 4.1 dieron forma al siguiente "cubo":



COBIT 4.1	COBIT 5
Efectividad	Utilidad
Eficiencia	Usabilidad
Integridad	Libre de error
Confiabilidad	Credibilidad
Disponibilidad	Accesibilidad
Confidencialidad	Seguridad
Cumplimiento	Conformidad

Figura 10. COBIT 4.1 criterios de formación

Modelo de Madurez:

A través del "Process Capability Model", COBIT 5 introduce un nuevo método de medir la madurez de los procesos, basado en el estándar internacional "ISO/IEC 15504 Software Engineering – Process Assessment Standard", con alguna variación tanto en el diseño como en el uso al modelo de madurez que incluía la versión anterior.

Figura 11. Modelo de madurez

Este nuevo modelo plantea las siguientes diferencias:

- El estándar ISO/IEC 15504 es más exigente debido a que plantea que se deben cumplir los 9 definidos para cada proceso, como requisito para acreditar dicho grado de madurez.
- De forma general, los resultados con estos niveles de madurez deberían de resultar más bajo.

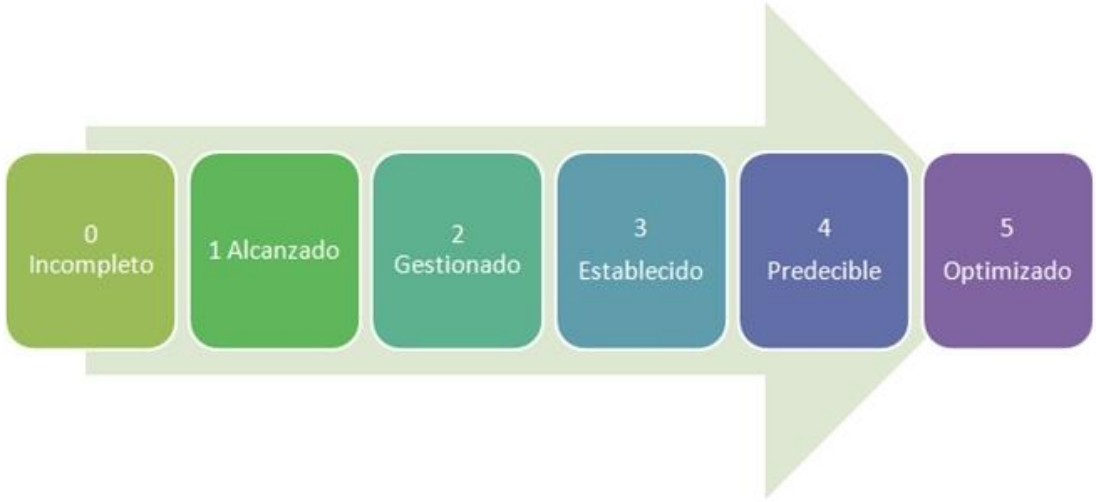


Figura 12. Estados del modelo de madurez

A continuación, se expone el mapeo oficial de ISACA entre ambos modelos de madurez:

COBIT 4.1	COBIT 5 ISO 15504	Contexto
5. Optimizado	5. Optimizado	Empresa / Conocimiento Corporativo
4. Gestionado	4. Predecible	
3. Definido	3. Establecido	
N/A	2. Gestionado	Individual / Conocimiento Individual
N/A	1. Alcanzado	
2. Repetible 1. Ad Hoc 0. No Existente	0. Incompleto	

Tabla 2. Mapeo oficial ISACA de COBIT 4.1 y COBIT 5

Conclusión del Comparativo

Es un marco de trabajo para llevar a cabo un mejor gerenciamiento de IT en relación al Gobierno de TI.

Con la nueva versión de COBIT se abre una nueva etapa para el gobierno y el management de TI, que implicará que todos los involucrados, más allá del rol (CEO, CIO, CRO, CISO, CCO, Advisor, Auditor, etc.), evolucionemos estratégicamente sincronizados con este nuevo estándar.

4.7.3 COBIT, COSO y el valor de los marcos de cumplimiento de SOX

COSO se encarga de la supervisión y da seguimiento a los equipos a implementar, mantener la información y la comunicación segura dentro de una organización, así mismo planea las actividades de control y la evaluación de los riesgos en un ambiente de control organizado.

Tres puntos importantes de los cuales se encarga COSO son:

1. Eficiencia Operativa
2. Cumplimiento Legal
3. Confiabilidad Financiera.

COBIT, plantea una alternativa o complementación de objetivos de control y organiza los requerimientos de la compañía en cuestión a las tecnologías de la información, así mismo es la adquisición e implementación de los mismos, se da entrega y soporte a los recursos informáticos y por ultimo mantiene la monitorización y el control de todos los recursos brindados de TI.

La implementación del COSO y COBIT es esencial para cualquier compañía que este en crecimiento, utilizando una planificación para los procesos de negocio y el control interno para mantener una producción más eficiente en cuanto a recursos de tecnología.

Cuando se implementa el COSO se da una planificación de los requerimientos de la compañía para tener eficiencia en las operaciones, se implementan los recursos informáticos cumpliendo con lo acordado durante la planificación y crear un ambiente de control en el cual se tenga la confiabilidad de que está generando ganancias financieras.

Cuando se implementa COBIT se cumplen los objetivos que se planearon durante el proceso del COSO y hace una revisión de la adquisición de los recursos informáticos, así mismo se implementan los recursos y se monitorean.

Control interno definió COSO como un proceso que es dirigido por un Consejo de administración, gestión y personal, para hacer una seguridad razonable en cuanto a; la eficacia y eficiencia de las operaciones, confiabilidad de la información financiera, cumplimiento de las leyes y reglamentos aplicables. Según el marco de control interno de COSO, que consta de cinco componentes interrelacionados, a saber: ambiente de Control, evaluación de riesgos, actividades de Control, información y comunicación, monitorización.

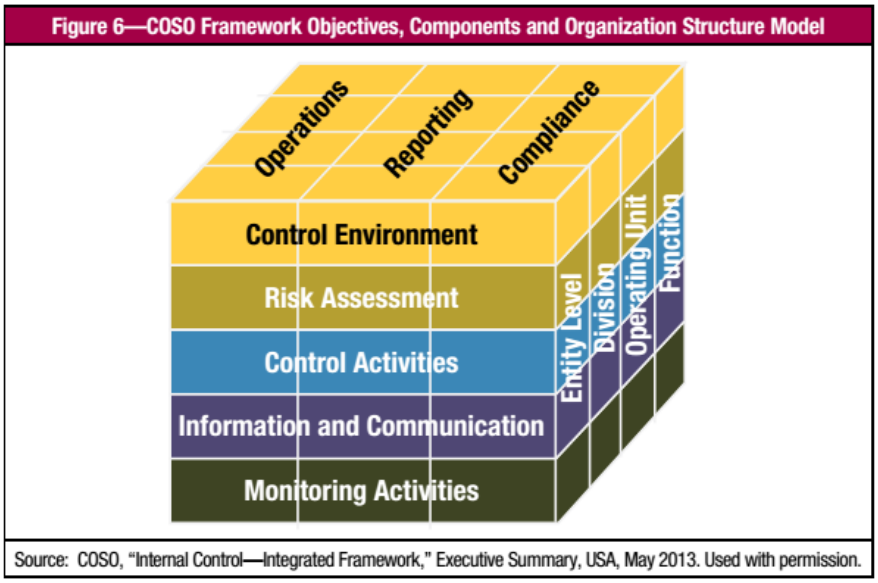


Figura 13. Objetivos del marco de trabajo COSO

El marco COSO define los objetivos de control sobre cada control a nivel de entidad que son constantemente utilizados como guía de la compañía para cumplir con la sección SOX 302 y 404. Sin embargo, COSO sólo proporciona una guía sobre el control extenso de la misma. En esta guía, COBIT 5 asigna a COSO muestra cómo los dos marcos son complementarios entre sí a los efectos de los requerimientos de SOX.

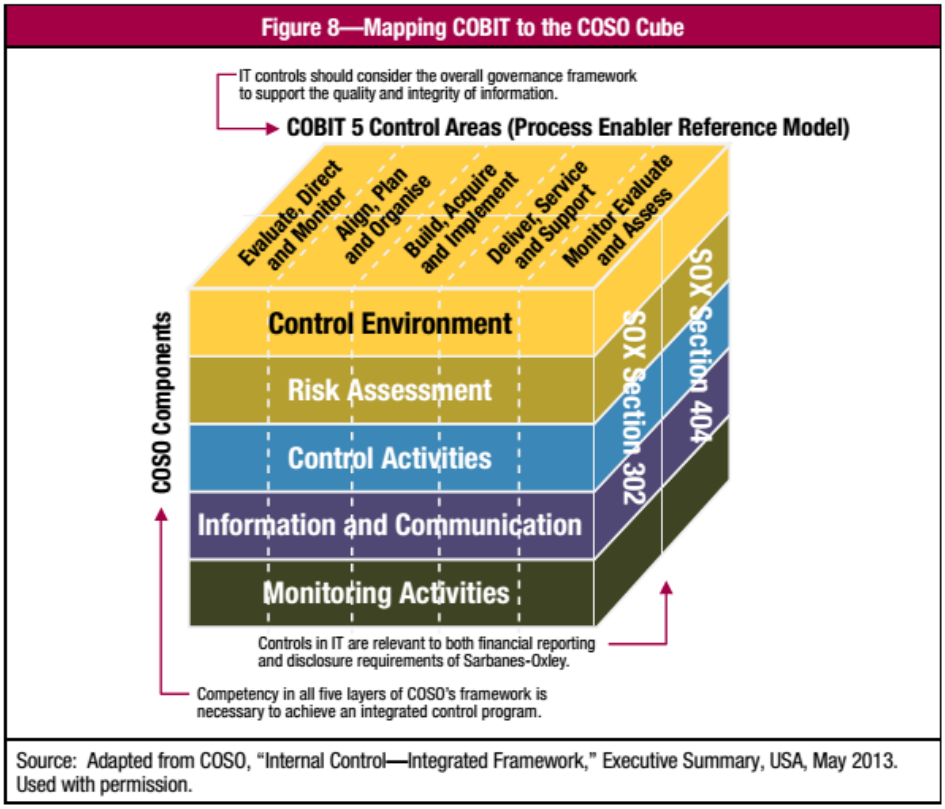


Figura 14. Mapeo COBIT vs cubo COSO

Siempre teniendo presente que la finalidad de estos marcos es conseguir que se cumpla la ley SOX, consistente en monitorear a las compañías que cotizan en bolsa, evitando que las acciones de las mismas sean alteradas de manera dudosa, mientras que su valor es menor. Tiene la finalidad de evitar fraudes y riesgos de bancarrota, protegiendo al inversor.

La primera y más importante parte de la ley establece una nueva agencia encargada de revisar, regular, inspeccionar y disciplinar a las auditorias. La ley también se refiere a la independencia de las auditorias, el gobierno corporativo y la transparencia financiera. Se considera uno de los cambios más significativos en la legislación empresarial.

CAPÍTULO 5

METODOLOGÍA PARA LA REVISIÓN DE CONTROLES GENERALES SOBRE SISTEMAS DE INFORMACIÓN

Sección 404 de la Sarbanes-Oxley Act of 2002

5. METODOLOGÍA PARA LA REVISIÓN DE CONTROLES GENERALES EN SISTEMAS DE INFORMACIÓN

La metodología que he considerado definir para la supervisión de los controles generales, como parte de objeto de este Proyecto, ha sido desarrollado teniendo en cuenta algunas referencias reconocidas a nivel internacional, entre otras el Informe COBIT (Control Objectives for Information and related Technology), siguiendo las recomendaciones de la ISACA (Information Systems Audit and Control Association). No obstante, se han considerado únicamente los objetivos de control necesarios para garantizar el cumplimiento de los requerimientos de la Sección 404 de la SOX sobre los controles generales sobre Sistemas de Información, ya que los objetivos del Informe COBIT exceden los requerimientos derivados de la citada Norma.

Dentro de los objetivos de control establecidos en el Informe COSO (eficacia y eficiencia de operaciones, fiabilidad de la Información Financiera, salvaguarda de activos y Cumplimiento de leyes y normas), se han considerado como objetivos del Modelo de Control Interno sobre el reporte financiero:

- Fiabilidad de la Información Financiera.
- Salvaguarda de Activos.
- Cumplimiento de Leyes y Normas en lo relativo a aquellas que afectan a la fiabilidad de la Información Financiera.

Para el desarrollo de la metodología de evaluación de controles generales sobre sistemas de información, he considerado entre otros los objetivos de control de COBIT que están orientados al cumplimiento de los anteriores objetivos, dejando al margen aspectos de este estándar que exceden el alcance de la metodología propuesta.

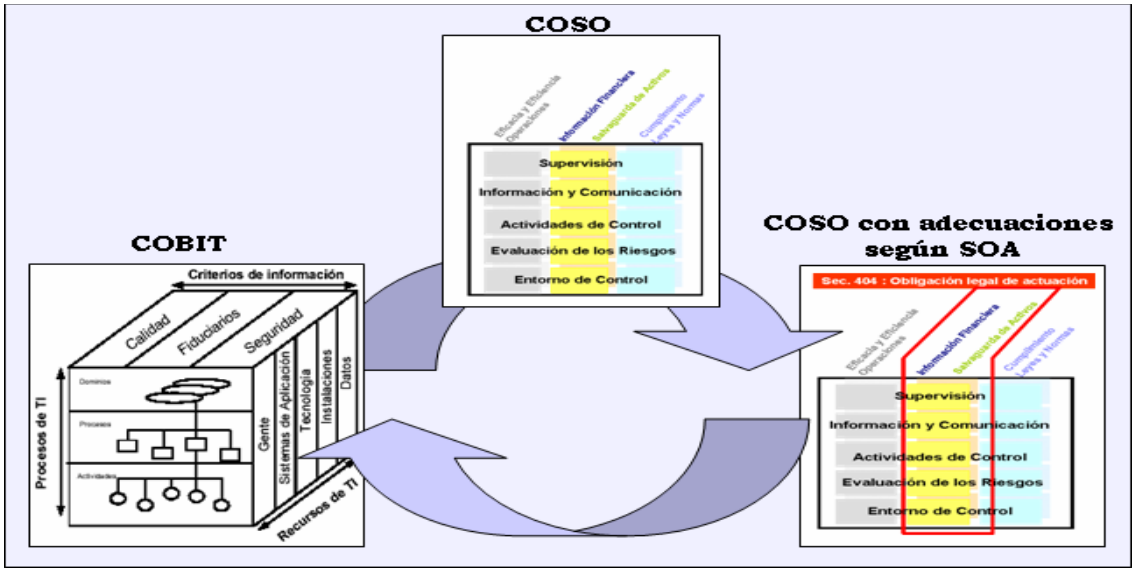


Figura 15. Relación COSO-COBIT y adaptación a los requerimientos de la Sección 404 de la ley Sarbanes-Oxley Act (SOX) o también conocido como SOA.

5.1 OBJETIVOS DE CONTROL

Los objetivos de control de los controles generales sobre sistemas de información, que forman parte del alcance de la evaluación según los requerimientos recogidos en la Sección 404 de la Ley Sarbanes-Oxley y conforme a las referencias metodológicas consideradas, son:

a) Seguridad Física
b) Seguridad Lógica
c) Explotación de Sistemas, también denominado como Operaciones
d) Desarrollo de Sistemas

El alcance definido en el apartado 3, considera la evaluación de los controles generales que afectan a las aplicaciones que soportan los procesos relevantes en las sociedades críticas identificadas a través del Modelo de definición de alcances.

En el Gráfico 3, se representa el alcance de los trabajos de evaluación: (i) los aspectos considerados (seguridad física, seguridad lógica, desarrollo de sistemas y explotación de sistemas) y (ii) la tipología general de los sistemas con impacto relevante en la información financiera (ERPs, Facturación, Sistemas de RR.HH y sistemas de consumo).

Figura 16. Alcance de la metodología desarrollada

Con objeto de facilitar la evaluación de los controles generales, a la hora de dar desarrollar la siguiente evaluación he establecido 3 grupos de objetivos generales, ya que seguridad lógica y seguridad física inicialmente lo incluimos dentro del grupo "Acceso a datos y sistemas". Para cada grupo de objetivos generales a evaluar se ha preparado una relación de objetivos específicos.

1. **Acceso a datos y sistemas** (Seguridad física y lógica)

   Se subdivide en los siguientes objetivos específicos:

   - Control de accesos sobre los programas.
   - Las aplicaciones de usuarios y el control sobre la manipulación.
   - El acceso a los datos.
   - El control sobre el acceso a los datos de las bases productivas.
   - Seguridad de los Centros de Procesamiento de Datos (CPD) e instalaciones, incluyendo las medidas de protección medioambiental.

Los riesgos que cubren estos objetivos son:

- Accesos físicos no autorizados.
- Ausencia/ exposición indebida de servicios generales de información.
- Daños accidentales/ intencionales de activos informáticos.
- Robo/ extracción de datos.
- Valores ambientales fuera de rango (T/H).
- Retrasos para la restauración de las operaciones.
- Gastos económicos no previstos.
- Infracciones ante el incumplimiento de obligaciones.
- Accesos no autorizados al sistema.
- Incidentes de seguridad sobre activos informáticos.
- Vulnerabilidades de seguridad en el software.
- Usuarios con privilegios indebidos sobre el sistema.
- Retrasos para la ejecución de acciones paliativas.
- Accesos lógicos no autorizados al sistema operativo.
- Accesos a archivos con información sensible.
- Utilización de servicios no seguros.
- Vínculos entre instalaciones operativas y de desarrollo.
- Facilidad de adivinación de contraseñas.

SEGURIDAD FÍSICA (AD-SF: Acceso a datos – Seguridad Física)

A continuación se muestran los controles detectados para la supervisión del acceso físico al CPD y las conclusiones que habría que obtener:

AD-SF-01. La petición de acceso es documentada y se indican claramente los datos generales de cada usuario así como los accesos a las distintas áreas restringidas

Solicitud formal de alta, baja o modificación en la que se indique claramente: usuario peticionario, usuario para el que se solicita acceso, área de acceso y periodo de acceso.

AD-SF-02. La petición de acceso está aprobada por parte del responsable.

Evidencia de aprobación formal de la solicitud (mediante firma manual o electrónica) por parte del responsable. La autorización deberá dejar registro del identificador y/o nombre del usuario que autoriza y de la fecha de autorización.

AD-SF-03. El acceso producido al CPD se registra adecuadamente (registro manual o electrónico).

Evidencia del acceso realizado por el usuario (mediante registro manual o electrónico), donde se detalle el identificador del usuario, área accedida, fecha y hora del acceso.

En caso de evidencia manual, verificar in situ que el acceso ha sido registrado.

AD-SF-04. Verificar que los usuarios que han accedido han sido previamente autorizados.

Se realizará un análisis de los accesos al CPD verificando que los mismos se corresponden con los que han sido autorizados.

- Listado o reporte de la totalidad de los usuarios que han accedido al CPD
- Listado o reporte de los usuarios autorizados a acceder al CPD.
- Cruce de los listados anteriores para verificar que los accesos producidos se corresponden con los usuarios autorizados.

AD-SF-05. Existe una revisión y actualización periódica de la lista de usuarios con acceso al CPD.

Evidencia de la última revisión de accesos al CPD realizada, la cual deberá cumplir con el procedimiento definido (en caso de que exista) y contener lo siguiente:

- Modo de realización de la revisión (en caso de que no exista procedimiento).
- Identificación del responsable de la revisión.
- Fecha de realización de la revisión.
- Evidencia de aprobación o no de los usuarios revisados con acceso al CPD.

SEGURIDAD LÓGICA (AD-SL: Acceso a datos – Seguridad Lógica)

1. GESTIÓN DE USUARIOS

A continuación se muestran los controles detectados así como las conclusiones que habría que obtener:

AD-SL-01. Existencia de una solicitud documentada de alta, baja o modificación de usuario.

Solicitud documentada del alta, baja o modificación en la que se indique claramente:

- Usuario peticionario.
- Usuario para el que se solicita acceso.
- Perfil solicitado.
- Aplicación afectada.

AD-SL-02. La solicitud ha sido autorizada por el responsable funcional.

Solicitud documentada que evidencie la aprobación (mediante firma manual o electrónica) del responsable funcional.

La autorización deberá haberse realizado antes de la creación/modificación de la cuenta de usuario y debe detallar el identificador y/o nombre del usuario y la fecha de autorización.

AD-SL-03. En caso de alta/modificación: el nivel de autorización especificado en la solicitud de acceso coincide con la autorización asignada en la aplicación.

Solicitud formal del alta, baja o modificación en la que se indique la autorización otorgada o perfil que contiene dicha autorización.

Reporte o captura de pantalla de la/s aplicación/es sobre las cual se otorgó acceso, en donde se evidencie el perfil asignado, así como las autorizaciones asociadas al mismo.

AD-SL-04. En caso de alta/modificación: El acceso concedido en la aplicación se corresponde con las funciones del usuario.

Identificar las funciones que lleva a cabo el usuario y verificar que las autorizaciones otorgadas se corresponden con sus funciones.

AD-SL-05. En caso de baja: el usuario no tiene acceso a la aplicación (deshabilitado o eliminado).

Reporte o captura de pantalla de la/s aplicación/es sobre la cual se deshabilitó o eliminó el usuario, en donde se evidencia que el usuario no existe o se encuentra deshabilitado o bloqueado.

2. CALIDAD DE LAS CONTRASEÑAS

AD-SL-06. Analizar la forma en que se crean y asignan las contraseñas para los usuarios de la aplicación y comprobar si es adecuada.

Verificar la parametrización de las contraseñas de la aplicación:

a) solicitud de cambio en el primer acceso
b) longitud mínima
c) caducidad de las contraseñas
d) número de intentos fallidos antes de bloqueo

Solicitar las evidencias relativas a los anteriores parámetros:

- Parametrización de la herramienta que gestiona las contraseñas.
- Capturas de pantalla del resultado tras los intentos de cambio de contraseña a cero caracteres y de pocos caracteres (un carácter menos que el mínimo).
- Capturas de pantalla del bloqueo de la cuenta de usuario tras intentar acceder de forma fallida.
- Correos de petición de cambio de contraseña por caducidad.

3. REVISIÓN PERIÓDICA DE USUARIOS

Los controles detectados y las conclusiones que se podrían obtener son los siguientes:

AD-SL-07. El administrador (o personal encargado de administrar los accesos) envía al responsable funcional un listado con las cuentas activas en el sistema y sus perfiles asociados.

Listado o reporte de cuentas activas en la aplicación enviado por el administrador al responsable funcional (o área responsable del proceso).

AD-SL-08. El responsable funcional analiza los usuarios dados de alta así como la adecuación de los perfiles configurados.

Evidencia de la revisión de usuarios por parte del responsable validando los perfiles asignados a cada uno de estos (correo / listado de usuarios con sus perfiles definitivos).

AD-SL-09. Una vez revisado el listado, el responsable funcional responde al administrador (o personal encargado de administrar los accesos) validando los usuarios o indicando las modificaciones necesarias.

Evidencia del análisis realizado por el responsable funcional (o área responsable del proceso), en la cual se verifiquen los hallazgos detectados y las medidas llevadas a cabo.

Comunicación formal de la respuesta del responsable funcional al administrador donde se detallan las validaciones realizadas sobre los usuarios analizados.

AD-SL-10. El administrador (o personal encargado de administrar los accesos) actualiza el sistema con las indicaciones recibidas del responsable funcional.

Listado o reporte de la aplicación, donde se detallen las cuentas activas en la aplicación con posterioridad al análisis realizado por el responsable funcional y las correcciones del administrador de la aplicación.

4. ANÁLISIS DE ALTOS PRIVILEGIOS DE USUARIOS

AD-SL-11. Verificar la razonabilidad de los usuarios con altos privilegios en la aplicación

Se considerarán usuarios con altos privilegios aquellos con permisos de administrador de la aplicación y aquellos con posibilidad de ejecutar transacciones o eventos críticos.

Se considerarán transacciones críticas aquellas determinadas por el responsable funcional de la aplicación.

Se realizará un análisis de los usuarios con altos privilegios en la aplicación y se verificará su razonabilidad junto con el responsable funcional de la aplicación.

Evidencia:

- Listado o reporte de la aplicación de la totalidad de los usuarios que cuentan con altos privilegios (Detallar: Identificador de usuario, nombre, perfil y autorización otorgada).
- Justificación de la razonabilidad de la asignación de dicho privilegio.

5. ANALISIS DE USUARIOS GENÉRICOS

AD-SL-12. Analizar el listado de usuarios y verificar la existencia de cuentas genéricas.

En caso de existir cuentas genéricas (es decir cuentas que no pueden vincularse con un único usuario) verificar lo siguiente:

- La cuenta no corresponde a una cuenta creada por defecto en la aplicación.
- En caso de tratarse de una cuenta creada por el administrador de la aplicación (o personal encargado de administrar los accesos), verificar si su existencia está debidamente justificada.

Evidencia:

- Listado de la totalidad de los usuarios de la aplicación.
- Identificación de los usuarios genéricos.
- Para los usuarios genéricos justificación de la necesidad de dicha cuenta.

6. PISTAS DE AUDITORÍA

A continuación se detallan los controles detectados además de las conclusiones que se deberían obtener:

AD-SL-13. El responsable funcional ha determinado qué evento de impacto en la información financiera (evento crítico) se va a recoger dentro de la pista de auditoría.

Listado de los eventos considerados por el responsable funcional que serán considerados en las pistas de auditoría.

AD-SL-14. Se han activado por la gerencia de seguridad informática (o personal encargado) las pistas de auditoría con las información financiera crítica solicitada por el responsable funcional.

Evidencia de la activación de las pistas de auditoría por parte del personal responsable. (Correo o evidencia donde se muestre la situación actual)

AD-SL-15. En la pista de auditoría se registra: fecha, nombre del usuario que ejecutó el proceso y el evento registrado.

Evidencia de que las pistas de auditoría (logs de eventos) se encuentran activadas en la aplicación.

Reporte de pistas de auditoría (logs de eventos) de la aplicación donde se especifique: fecha del registro, usuario que ejecuta el evento, evento registrado.

AD-SL-16. El responsable funcional (o personas en las que delega) revisa periódicamente el listado de pistas de auditoría de la aplicación. Este atributo no aplica en aquellos casos en los cuales el log es revisado tras la ocurrencia de un incidente (como control de detección).

Evidencia de la revisión de eventos realizada por el responsable funcional y de la comunicación de las anomalías detectadas.

7. SEGREGACIÓN DE FUNCIONES DE USUARIOS ADMINISTRADORES

AD-SL-17. Verificar que el personal encargado de la administración de usuarios no tiene acceso a transacciones incompatibles con sus funciones o innecesarias para la labor que realizan.

Se verificará que los Administradores de usuarios de la aplicación no pueden ejecutar transacciones de operación de la aplicación, ni acceder como usuarios finales a la misma.

En caso de presentarse diferencias, deberá existir una justificación por parte del Responsable funcional de la aplicación.

Evidencia:

- Documento formal en el cual se detallen los nombres de la totalidad de los administradores de usuarios de la aplicación, área a la cual pertenecen y funciones que desempeñan.
- Documento de los perfiles en la aplicación donde se evidencia que los mismos no permiten realizar tareas incompatibles con sus funciones.

En caso de excepciones, se solicitará al responsable funcional una justificación de las mismas.

2. OPERACIONES – EXPLOTACIÓN DE SISTEMAS (OP: Operaciones).

Se subdivide en los siguientes objetivos específicos:

- Salvaguarda de información (Backup)
- Tareas no programadas
- Gestión de incidencias
- Gestión de cambios de infraestructura

Los riesgos que cubren estos objetivos son:

- Acceso/ alteración indebida de programas fuente.
- Implementación injustificada de cambios.
- Desarrollos no alineados a los estándares.
- Programas productivos con funcionalidad no probada.
- Accesos lógicos.

- Pérdida de CID en las salidas de datos.
- Enlaces entre instalaciones operativas y de desarrollo.
- Ausencia de trazabilidad.

1. SALVAGUARDA DE INFORMACIÓN: BACKUP (OP-BA: Operaciones – Backup)

A continuación se muestran los controles detectados para el procedimiento de gestión de backups y las conclusiones que se deberían obtener:

OP-BA-01. La copia de seguridad contiene los ficheros de la aplicación.

Evidencia de que la herramienta de gestión de backups, recoge los datos de la aplicación y base de datos de los que se va a realizar la copia de seguridad.

OP-BA-02. El proceso copia de seguridad ha finalizado correctamente. Verificar que el soporte de copia de seguridad no ha superado su vida útil.

Evidencia de la finalización correcta de la realización de la copia de seguridad, así como el número de usos de la cinta (soporte) y antigüedad de la misma.

OP-BA-03. La copia de seguridad está almacenada correctamente (lugar identificable y fácilmente ubicable).

Evidencia del almacenamiento de la cinta (soporte), reflejando ubicación física de la misma.

OP-BA-04. En caso de error, éste queda registrado, se analiza el motivo y se corrige.

Evidencia de la finalización incorrecta de la copia de seguridad, así como de las acciones que se han llevado a cabo para corregir esta acción, para que no se vuelva a dar este error.

2. TAREAS PROGRAMADAS: PROCESOS BATCH (OP-PB: Operaciones – Procesos Batch)

Los controles detectados para el procedimiento de planificación de tareas programadas así como las conclusiones se detallan a continuación:

OP-PB-01. Existe una solicitud de planificación de tarea.

Evidencia de la solicitud de planificación de la tarea.

OP-PB-02. Existe una autorización para la ejecución de la tarea programada.

Evidencia de la autorización para la implementación de la tarea programada.

OP-PB-03. La tarea planificada ha terminado correctamente.

Evidencia de la finalización correcta de la tarea programada, verificando el resultado satisfactorio de la misma así como el tiempo de inicio, fin y duración de la tarea.

OP-PB-04. En caso de haberse producido una ejecución incorrecta de la tarea planificada, acciones tomadas para la solución del error.

Evidencia del registro de la finalización incorrecta de la tarea programada, así como de las medidas tomadas para la reejecución y solución de la tarea ejecutada incorrectamente.

Debe recogerse además:

- Usuario/s que las realizaron
- Finalización de la reejecución de la tarea (correcta /incorrecta)
- Duración de la reejecución
- Inicio y fin de la tarea reejecutada.

OP-PB-05. Existe una adecuada segregación de funciones entre los responsables de la gestión de las tareas programadas.

Evidencia de la existencia de una adecuada segregación de funciones. Incluir evidencias de la revisión realizada con el personal de desarrollo.

3. GESTIÓN DE INCIDENCIAS (OP-GI: Operaciones – Gestión de Incidencias)

Los controles detectados para el procedimiento de incidencias se muestran a continuación junto con las conclusiones que se obtendrían:

OP-GI-01. Existencia de solicitud de apertura de incidencia.

Verificar que existe una correcta identificación del usuario/cliente que abre la incidencia

Evidencia de la apertura de la incidencia indicando claramente la fecha y la hora de la realización de la apertura de la misma.

OP-GI-02. Verificar que se pueden identificar la aplicación/plataforma afectada por la incidencia.

Verificar que existe un detalle explicativo conciso de la incidencia en su entrada en el sistema.

OP-GI-03. Determinar que la incidencia ha sido priorizada.

Evidencia de que la incidencia está clasificada por su prioridad (alta, baja, grave, media, absoluta, etc.).

OP-GI-04. Verificar que la incidencia ha sido cerrada.

Evidencia de que la incidencia ha sido resuelta, indicando las medidas realizadas para solventarla, quien ha realizado las acciones para solventarla, fecha de realización de dichas acciones.

OP-GI-05. Verificar que la resolución de la incidencia ha sido comunicada al usuario que la originó.

Evidencia de que la resolución de la incidencia ha sido notificada al usuario que abrió la incidencia, así como la aceptación de éste de la resolución.

OP-GI-06. Existencia de un proceso de monitorización de las incidencias abiertas.

Evidenciar cómo se realiza la monitorización de las incidencias, indicando qué acciones se realizan para el cierre de las incidencias abiertas.

4. GESTIÓN DE CAMBIOS A INFRAESTRUCTURA (OP-GCI: Operaciones – Gestión de cambios a infraestructura)

Los controles detectados para el procedimiento de cambios a infraestructura y conclusiones que se obtendrían son:

OP-GCI-01. Existe una solicitud que describe la naturaleza, prioridad y la justificación del cambio.

A partir del registro de cambios de infraestructura implementados en el entorno de producción, seleccionar la evidencia de una solicitud de requerimiento por parte del área usuaria o del área técnica. (Correo electrónico, hoja de cálculo, aplicación específica).

Verificar la existencia de:

- Sistema afectado
- Peticionario del cambio
- Descripción del cambio dependiendo de la naturaleza del mismo:
    - Nueva infraestructura
    - Modificación/Mejora
- Fecha de solicitud.
- Identificativo del cambio que se va a realizar para poder realizar un seguimiento del mismo.

OP-GCI-02. El cambio ha sido probado en un entorno de pruebas/certificación (pre-producción)

Evidencia de ejecución de pruebas asociadas a los cambios de infraestructura antes de su implantación en el entorno de producción:

- Verificar que existe un plan de pruebas y evidencia resultado de la aplicación del plan de pruebas.
- Verificar que existe un procedimiento de marcha atrás o rollback.

OP-GCI-03. El responsable correspondiente ha autorizado implementación en producción del cambio solicitado.

Evidencia de la autorización del traspaso al entorno de producción

- Verificar que la autorización del paso a producción se realiza por el responsable correspondiente (mail / listado con los usuarios autorizados).

OP-GCI-04. La puesta en producción ha sido realizada por el personal técnico adecuado.

Identificación de que existen distintos entornos a la hora de realizar los cambios de infraestructura.

Evidencia de quién ha realizado la implementación de los cambios en el entorno de producción: personal técnico correspondiente.

Verificación de que el Responsable que autoriza el cambio no sea el mismo que quien ha realizado la implementación en el entorno de producción.

3. DESARROLLO DE SISTEMAS - CAMBIOS A PROGRAMAS (CP: Cambios a programas)

Se subdivide en los siguientes objetivos específicos:

- Metodología de desarrollo y mantenimiento de sistemas
- Pasos metodológicos para las aplicaciones
- Flujo de aprobaciones
- Toma de requisitos del sistema
- Pruebas de aplicaciones

Los riesgos que cubren estos objetivos son:

- Acceso/ alteración indebida de programas fuente.
- Implementación injustificada de cambios.
- Desarrollos no alineados a los estándares.
- Programas productivos con funcionalidad no probada.

A continuación se muestran los controles detectados para el procedimiento de cambios a programas y las conclusiones que habría que obtener:

CP-01. Existe una solicitud que describe la naturaleza y la extensión del cambio.

A partir del registro de los cambios implantados en el entorno productivo, seleccionar evidencia de una solicitud del área usuaria o del área técnica formalizada de requerimiento de cambio a programa. (Correo electrónico, hoja de cálculo, aplicación específica, etc.).

Verificar la existencia de:

- Aplicación afectada

- Peticionario del cambio
- Descripción del cambio dependiendo de la naturaleza del mismo:
    - Nuevo desarrollo
    - Modificación/Mejora
    - Cambio de emergencia
- Fecha de solicitud.
- Identificativo del cambio que se va a realizar para poder realizar un seguimiento del mismo.

CP-02. El responsable correspondiente ha autorizado el desarrollo del cambio solicitado.

Evidencia de que la solicitud del cambio ha sido aprobada por el área correspondiente:

- Verificar que el aprobador es el responsable del sistema o un usuario autorizado para aprobar desarrollos (existencia de una lista de aprobadores)

CP-03. El cambio ha sido probado por el área usuaria en un entorno de pruebas/certificación.

Evidencia de que el área usuaria o el área técnica realizan las pruebas a los cambios a programas antes de su implantación:

- Verificar que existe un plan de pruebas y documento resultado de la aplicación del plan de pruebas.

CP-04. El área usuaria acepta el resultado de las pruebas.

Evidencia de la aceptación del cambio.

- Verificar que la aceptación se realiza por el área usuaria/técnica (en caso de ser un cambio iniciado por Sistemas de Información)

CP-05. El responsable correspondiente ha autorizado el paso a producción del cambio solicitado.

Evidencia de la autorización del traspaso del objeto al entorno de producción

- Verificar que la autorización del paso a producción se realiza por el responsable del sistema (correo / listado con los usuarios autorizados).

CP-06. El objeto ha sido pasado al entorno de producción por el personal autorizado no correspondiente al área de desarrollo.

Identificación de que existen distintos entornos a la hora de realizar los cambios a programas.

Evidencia de quien ha realizado el paso de los cambios en el entorno de producción.

Verificar que:

- El paso a producción lo realiza una persona adecuada (No pertenece al área de desarrollo).

- Si se emplean herramientas o aplicaciones para los pases de desarrollos al entorno de producción, identificar a través de la herramienta qué usuario ha realizado el pase.

CP-07. Monitorización del proceso de gestión de cambios a programas.

Evidencia de la existencia de un comité de cambios y de que se revisan los cambios pasados a producción.

CAPÍTULO 6

MARCO DE EVALUACIÓN

6. MARCO DE EVALUACIÓN

En este capítulo se estudiaran las diferentes preguntas/respuestas que se tendrán en cuenta para indicar la confianza en los sistemas en la aplicación a desarrollar.

A continuación se mostrará y explicare la plantilla que he seguido para plasmar la marco de evaluación creada para dicha aplicación. Esta plantilla contendrá el riesgo, el control, la pregunta y sus diferentes respuestas y las diversas recomendaciones que se le aplican a las compañías conforme a SOX 404.

Tras el repertorio de cuestiones se explicara de forma precisa y detallada la evaluación en cuestión.

<table>
<tr><td colspan="2">TITULO DEL ÁREA</td></tr>
<tr><td colspan="2">TITULO CONTROL</td></tr>
<tr><td colspan="2">PREGUNTA "N"</td></tr>
<tr><td colspan="2">Enunciado de la pregunta en cuestión</td></tr>
<tr><td colspan="2">VALORACIONES</td></tr>
<tr><td>Respuesta 1</td><td>"Respuesta 1" -> Pregunta Siguiente
* Recomendación en caso de ser la respuesta incorrecta.</td></tr>
<tr><td colspan="2">....</td></tr>
<tr><td>Respuesta N</td><td>"Respuesta N" -> Pregunta Siguiente
* Recomendación en caso de ser la respuesta incorrecta.</td></tr>
<tr><td colspan="2">COMENTARIOS</td></tr>
<tr><td colspan="2">Comentarios que ayudan a reconocer el porqué de la respuesta correcta en cada pregunta.</td></tr>
</table>

- Las recomendaciones que aparecen serán aquellas que formaran el futuro dossier de recomendaciones para cada compañía que solucione el cuestionario.

Aspectos a tener en cuenta:

Aplicación “X”: Las preguntas de la 6 a la 23 se van a realizar para cada una de las aplicaciones en el alcance, es decir, que tengan incidencia en los estados financieros.

Sistema operativo “Y”: Las preguntas de la 24 a la 41 se van a realizar para cada una de los servidores (sistemas operativos) donde se aloja cada aplicación en el alcance.

Base de datos “Z”: Las preguntas de la 42 a la 59 se van a realizar para cada una de las bases de datos que soportan cada aplicación en el alcance.

Matriz de muestras: Las preguntas en las que se indica “Para toda la población muestreada” tienen como significado que la respuesta de estas preguntas sea la respuesta final tras cumplir con cada pregunta para toda la muestra.

Como extraer la muestra de la población total: En la siguiente tabla se indica el número de ítems que deberán seleccionarse basándose en la frecuencia del control o en la población total. Podemos comprobar que en algunos casos aparecen varios valores, esto va a depender del grado de control que consideremos que tienen los sistemas, si es la primera vez que se realiza se recomienda recurrir al máximo o en caso de que se haya realizado la revisión en el año anterior y haya ocurrido alguna incidencia en relación a esa área.

Frequency of control	Assumed population of controls occurrences	Number of items to test
Annual	1	1
Quarterly	4	2
Monthly	12	2 to 5
Weekly	52	5, 10, 15
Daily	250	20, 30, 40
Multiple times per day	Over 250	25, 45, 60

6.1 ACCESO A DATOS Y SISTEMAS (SEGURIDAD FÍSICA Y LÓGICA)

Dentro de este grupo se incluyen los objetivos específicos relacionados con seguridad física y lógica. Estos controles y sus correspondientes actividades cubren aspectos como control de accesos a los sistemas, control sobre las cuentas privilegiadas, control de trazabilidad de las acciones que se realizan sobre los mismos, etc.

SEGURIDAD FÍSICA	
CONTROL DE ACCESOS	
PREGUNTA 1	
Existe una petición de acceso documentada donde se indican claramente los datos generales de cada usuario así como los accesos a las distintas áreas restringidas	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 2
Respuesta 2	No -> Es recomendable que exista una petición que recoja los datos generales de cada usuario que accede a las zonas restringidas.
COMENTARIOS	
Según la sección 404 de SOX es recomendable mantener un control de los accesos de los usuarios que acceden a las zonas restringidas (CPD).	

SEGURIDAD FÍSICA	
CONTROL DE ACCESOS	
PREGUNTA 2	
La petición se encuentra revisada y aprobada por el responsable funcional	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable que la petición además de existir se encuentra revisada y aprobada por el responsable funcional.
COMENTARIOS	
Según la sección 404 de SOX es recomendable mantener un control de los accesos de los usuarios que acceden a las zonas restringidas (CPD).	

SEGURIDAD FÍSICA	
CONTROL DE ACCESOS	
PREGUNTA 3	
Existe un registro de los accesos producidos al CPD (registro manual o electrónico).	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 4
Respuesta 2	No -> Es recomendable mantener un registro de los accesos producidos al CPD.
COMENTARIOS	
Según la sección 404 de SOX es recomendable mantener un control de los accesos de los usuarios que acceden a las zonas restringidas (CPD).	

SEGURIDAD FÍSICA	
CONTROL DE ACCESOS	
PREGUNTA 4	
Los usuarios que han accedido han sido previamente autorizados.	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable que los accesos registrados correspondan a usuarios autorizados.
COMENTARIOS	
Según la sección 404 de SOX es recomendable mantener un control de los accesos de los usuarios que acceden a las zonas restringidas (CPD).	

SEGURIDAD FÍSICA	
CONTROL DE ACCESOS	
PREGUNTA 5	
Existe una revisión y actualización periódica de la lista de usuarios con acceso al CPD.	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable realizar revisiones con periodicidad para evitar accesos de usuarios indebidos.
COMENTARIOS	
Según la sección 404 de SOX es recomendable mantener un control de los accesos de los usuarios que acceden a las zonas restringidas (CPD).	

SEGURIDAD LÓGICA	
CONTROL DE ACCESOS	
PREGUNTA 6	
Existencia de un procedimiento de gestión de usuarios a nivel de la aplicación “X” que describa las distintas etapas del proceso así como las personas responsables.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 7
Respuesta 2	No -> Es recomendable que exista un procedimiento a nivel de aplicación que recoja el detalle del proceso y las personas responsables
COMENTARIOS	
Según la sección 404 de SOX es recomendable mantener un procedimiento formalizado que recoja el detalle del proceso de gestión a nivel de aplicación que será utilizado en el momento de ejecutar las solicitudes.	

SEGURIDAD LÓGICA	
CONTROL DE ACCESOS	
PREGUNTA 7	
Existencia de una solicitud documentada de alta, baja o modificación de usuario de la aplicación “X”.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 8
Respuesta 2	No -> Es recomendable que exista una petición que recoja los datos de los usuarios así como los permisos que se solicitan en la aplicación.
COMENTARIOS	
Según la sección 404 de SOX es recomendable mantener un control de gestión de los usuarios con acceso a las aplicaciones.	

SEGURIDAD LÓGICA	
CONTROL DE ACCESOS	
PREGUNTA 8	
La petición del usuario de la aplicación “X” se encuentra revisada y aprobada por el responsable funcional.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 9
Respuesta 2	No -> Es recomendable que la petición además de existir se encuentra revisada y aprobada por el responsable funcional.
COMENTARIOS	
Según la sección 404 de SOX es recomendable mantener un control de gestión de los usuarios con acceso a las aplicaciones.	

SEGURIDAD LÓGICA	
CONTROL DE ACCESOS	
PREGUNTA 9	
En caso de alta/modificación: el nivel de autorización especificado en la solicitud de acceso coincide con la autorización asignada en la aplicación “X”.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 10
Respuesta 2	No -> Es recomendable este autorizada por el responsable funcional autorizado en la aplicación.
COMENTARIOS	
Según la sección 404 de SOX es recomendable mantener un control de gestión de los usuarios con acceso a las aplicaciones.	

SEGURIDAD LÓGICA	
CONTROL DE ACCESOS	
PREGUNTA 10	
En caso de alta/modificación: El acceso concedido en la aplicación “X” se corresponde con las funciones del usuario	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable que el usuario dado de alta/modificado cuente con el permiso acorde a sus funciones.
COMENTARIOS	
Según la sección 404 de SOX es recomendable mantener un control de gestión de los usuarios con acceso a las aplicaciones.	

SEGURIDAD LÓGICA	
CONTROL DE ACCESOS	
PREGUNTA 11	
En caso de baja: el usuario no tiene acceso a la aplicación (deshabilitado o eliminado) “X”.	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable dar de baja o deshabilitar el usuario en tiempo y forma en la aplicación.
COMENTARIOS	
Según la sección 404 de SOX es recomendable mantener un control de gestión de los usuarios con acceso a las aplicaciones.	

SEGURIDAD LÓGICA	
CALIDAD DE LAS CONTRASEÑAS	
PREGUNTA 12	
Analizar la forma en que se crean y asignan las contraseñas para los usuarios de la aplicación “X” y comprobar si es adecuada a) solicitud de cambio en el primer acceso b) longitud mínima c) caducidad de las contraseñas d) número de intentos fallidos antes de bloqueo	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable definir los parámetros de forma razonable y adecuada.
COMENTARIOS	
Según la sección 404 de SOX es recomendable mantener una configuración de seguridad adecuada en las aplicaciones.	

SEGURIDAD LÓGICA	
REVISIÓN PERIÓDICA DE USUARIOS	
PREGUNTA 13	
El administrador (o personal encargado de administrar los accesos) envía al responsable funcional un listado con las cuentas activas en el sistema y sus perfiles asociados en la aplicación “X”.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 14
Respuesta 2	No -> Es recomendable mantener una segregación de funciones que se encarguen de revisar los usuarios y proceder a realizar las acciones necesarias.
COMENTARIOS	
Según la sección 404 de SOX es recomendable realizar una revisión periódica de usuarios de cada aplicación, ejecutada por el administrador e indicada por el responsable.	

SEGURIDAD LÓGICA	
REVISIÓN PERIÓDICA DE USUARIOS	
PREGUNTA 14	
El responsable funcional analiza los usuarios dados de alta así como la adecuación de los perfiles configurados en la aplicación “X”.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 15
Respuesta 2	No -> Es recomendable mantener una segregación de funciones que se encarguen de revisar los usuarios y proceder a realizar las acciones necesarias.
COMENTARIOS	
Según la sección 404 de SOX es recomendable realizar una revisión periódica de usuarios de cada aplicación, ejecutada por el administrador e indicada por el responsable.	

SEGURIDAD LÓGICA	
REVISIÓN PERIÓDICA DE USUARIOS	
PREGUNTA 15	
Una vez revisado el listado, el responsable funcional responde al administrador (o personal encargado de administrar los accesos) validando los usuarios o indicando las modificaciones necesarias para la aplicación “X”.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 16
Respuesta 2	No -> Es recomendable mantener una segregación de funciones que se encarguen de revisar los usuarios y proceder a realizar las acciones necesarias.
COMENTARIOS	
Según la sección 404 de SOX es recomendable realizar una revisión periódica de usuarios de cada aplicación, ejecutada por el administrador e indicada por el responsable.	

SEGURIDAD LÓGICA	
REVISIÓN PERIÓDICA DE USUARIOS	
PREGUNTA 16	
El administrador (o personal encargado de administrar los accesos) actualiza en la aplicación “X” con las indicaciones recibidas del responsable funcional.	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable mantener una segregación de funciones que se encarguen de revisar los usuarios y proceder a realizar las acciones necesarias.
COMENTARIOS	
Según la sección 404 de SOX es recomendable realizar una revisión periódica de usuarios de cada aplicación, ejecutada por el administrador e indicada por el responsable.	

SEGURIDAD LÓGICA	
ALTOS PRIVILEGIOS DE USUARIOS	
PREGUNTA 17	
Los usuarios con altos privilegios se encuentran asignados en la aplicación de forma razonable y coherente de acuerdo a las funciones en la aplicación “X”.	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable que los usuarios con altos privilegios se encuentren correctamente asignados a los usuarios.
COMENTARIOS	
Según la sección 404 de SOX es recomendable limitar los usuarios con altos privilegios al menor número de personas dado que mantienen la posibilidad de ejecutar transacciones críticas en la aplicación.	

SEGURIDAD LÓGICA	
ALTOS PRIVILEGIOS DE USUARIOS	
PREGUNTA 18	
Verificar que el personal encargado de la administración de usuarios en la aplicación “X” no tiene acceso a transacciones incompatibles con sus funciones o innecesarias para la labor que realizan.	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable que los usuarios con altos privilegios se encuentren correctamente segregados de la ejecución de acciones con incidencia contable.
COMENTARIOS	
Según la sección 404 de SOX es recomendable que exista una correcta segregación de funciones entre la administración y la ejecución de transacciones de operación de la aplicación.	

SEGURIDAD LÓGICA	
CUENTAS GENÉRICAS DE USUARIO	
PREGUNTA 19	
Las cuentas genéricas, en caso de existir, pertenecen a cuentas por defecto de la aplicación "X" o se encuentran debidamente justificadas.	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable mantener un control de las cuentas genéricas y de las funciones que se realizan con las mismas.
COMENTARIOS	
Según la sección 404 de SOX es recomendable que las cuentas genéricas se encuentren controladas en la aplicación.	

SEGURIDAD LÓGICA	
PISTAS DE AUDITORÍA	
PREGUNTA 20	
El responsable funcional ha determinado qué evento tiene impacto en la información financiera (evento crítico) y se va a recoger dentro de la pista de auditoría de la aplicación "X".	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 21
Respuesta 2	No -> Es recomendable definir los eventos considerados críticos en la aplicación.
COMENTARIOS	
Según la sección 404 de SOX es recomendable registrar en la aplicación los eventos críticos que puedan repercutir contablemente de algún modo.	

SEGURIDAD LÓGICA	
PISTAS DE AUDITORÍA	
PREGUNTA 21	
Se han activado por la gerencia de seguridad informática (o personal encargado) las pistas de auditoría con las información financiera crítica solicitada por el responsable funcional en la aplicación “X”.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 22
Respuesta 2	No -> Es recomendable activar las trazas de auditoría con la información financiera crítica.
COMENTARIOS	
Según la sección 404 de SOX es recomendable registrar en la aplicación los eventos críticos que puedan repercutir contablemente de algún modo.	

SEGURIDAD LÓGICA	
PISTAS DE AUDITORÍA	
PREGUNTA 22	
En la pista de auditoría se registra: fecha, nombre del usuario que ejecutó el proceso y el evento registrado para la aplicación “X”.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 23
Respuesta 2	No -> Es recomendable almacenar la información necesaria para identificar los eventos.
COMENTARIOS	
Según la sección 404 de SOX es recomendable registrar en la aplicación los eventos críticos que puedan repercutir contablemente de algún modo.	

SEGURIDAD LÓGICA	
PISTAS DE AUDITORÍA	
PREGUNTA 23	
El responsable funcional (o personas en las que delega) revisa periódicamente el listado de pistas de auditoría de la aplicación "X". Este atributo no aplica en aquellos casos en los cuales el log es revisado tras la ocurrencia de un incidente (como control de detección).	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable revisar y mantener un control de los listados de auditoría registrados en la aplicación.
COMENTARIOS	
Según la sección 404 de SOX es recomendable revisar los eventos críticos de la aplicación que puedan repercutir contablemente de algún modo.	

SEGURIDAD LÓGICA	
CONTROL DE ACCESOS	
PREGUNTA 24	
Existencia de un procedimiento de gestión de usuarios a nivel de sistema operativo que describa las distintas etapas del proceso así como las personas responsables.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 25
Respuesta 2	No -> Es recomendable que exista un procedimiento a nivel de sistema operativo que recoja el detalle del proceso y las personas responsables de cada etapa.
COMENTARIOS	
Según la sección 404 de SOX es recomendable mantener un procedimiento formalizado que recoja el detalle del proceso de gestión a nivel de sistema operativo que será utilizado en el momento de ejecutar las solicitudes.	

SEGURIDAD LÓGICA	
CONTROL DE ACCESOS	
PREGUNTA 25	
Existencia de una solicitud documentada de alta, baja o modificación de usuario del servidor (sistema operativo) “Y”.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 26
Respuesta 2	No -> Es recomendable que exista una petición que recoja los datos de los usuarios así como los permisos que se solicitan en el sistema operativo.
COMENTARIOS	
Según la sección 404 de SOX es recomendable mantener un control de gestión de los usuarios con acceso a los sistemas operativos.	

SEGURIDAD LÓGICA	
CONTROL DE ACCESOS	
PREGUNTA 26	
La petición del usuario del servidor (sistema operativo) “Y” se encuentra revisada y aprobada por el responsable funcional.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 27
Respuesta 2	No -> Es recomendable que la petición además de existir se encuentra revisada y aprobada por el responsable funcional.
COMENTARIOS	
Según la sección 404 de SOX es recomendable mantener un control de gestión de los usuarios con acceso a los sistemas operativos.	

SEGURIDAD LÓGICA	
CONTROL DE ACCESOS	
PREGUNTA 27	
En caso de alta/modificación: el nivel de autorización especificado en la solicitud de acceso coincide con la autorización asignada en el servidor (sistema operativo) “Y”	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 28
Respuesta 2	No -> Es recomendable este autorizada por el responsable funcional autorizado en el sistema operativo.
COMENTARIOS	
Según la sección 404 de SOX es recomendable mantener un control de gestión de los usuarios con acceso a los sistemas operativos.	

SEGURIDAD LÓGICA	
CONTROL DE ACCESOS	
PREGUNTA 28	
En caso de alta/modificación: El acceso concedido en el servidor (sistema operativo) “Y” se corresponde con las funciones del usuario	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable que el usuario dado de alta/modificado cuente con el permiso acorde a sus funciones.
COMENTARIOS	
Según la sección 404 de SOX es recomendable mantener un control de gestión de los usuarios con acceso a los sistemas operativos.	

SEGURIDAD LÓGICA	
CONTROL DE ACCESOS	
PREGUNTA 29	
En caso de baja: el usuario no tiene acceso al servidor (sistema operativo) “Y” (deshabilitado o eliminado).	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable dar de baja o deshabilitar el usuario en tiempo y forma en la aplicación.
COMENTARIOS	
Según la sección 404 de SOX es recomendable mantener un control de gestión de los usuarios con acceso a los sistemas operativos.	

SEGURIDAD LÓGICA	
CALIDAD DE LAS CONTRASEÑAS	
PREGUNTA 30	
Analizar la forma en que se crean y asignan las contraseñas para los usuarios del servidor (sistema operativo) “Y” y comprobar si es adecuada a) solicitud de cambio en el primer acceso b) longitud mínima c) caducidad de las contraseñas d) número de intentos fallidos antes de bloqueo	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable definir los parámetros de forma razonable y adecuada en el sistema operativo
COMENTARIOS	
Según la sección 404 de SOX es recomendable mantener una configuración de seguridad adecuada en los sistemas operativos.	

SEGURIDAD LÓGICA	
REVISIÓN PERIÓDICA DE USUARIOS	
PREGUNTA 31	
El administrador (o personal encargado de administrar los accesos) envía al responsable funcional un listado con las cuentas activas en el sistema y sus perfiles asociados en el servidor (sistema operativo) “Y”	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 32
Respuesta 2	No -> Es recomendable mantener una segregación de funciones que se encarguen de revisar los usuarios y proceder a realizar las acciones necesarias.
COMENTARIOS	
Según la sección 404 de SOX es recomendable realizar una revisión periódica de usuarios de cada sistema operativo, ejecutada por el administrador e indicada por el responsable.	

SEGURIDAD LÓGICA	
REVISIÓN PERIÓDICA DE USUARIOS	
PREGUNTA 32	
El responsable funcional analiza los usuarios dados de alta así como la adecuación de los perfiles configurados en el servidor (sistema operativo) “Y”.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 33
Respuesta 2	No -> Es recomendable mantener una segregación de funciones que se encarguen de revisar los usuarios y proceder a realizar las acciones necesarias.
COMENTARIOS	
Según la sección 404 de SOX es recomendable realizar una revisión periódica de usuarios de cada sistema operativo, ejecutada por el administrador e indicada por el responsable.	

SEGURIDAD LÓGICA	
REVISIÓN PERIÓDICA DE USUARIOS	
PREGUNTA 33	
Una vez revisado el listado, el responsable funcional responde al administrador (o personal encargado de administrar los accesos) validando los usuarios o indicando las modificaciones necesarias para el servidor (sistema operativo) "Y".	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 34
Respuesta 2	No -> Es recomendable mantener una segregación de funciones que se encarguen de revisar los usuarios y proceder a realizar las acciones necesarias.
COMENTARIOS	
Según la sección 404 de SOX es recomendable realizar una revisión periódica de usuarios de cada sistema operativo, ejecutada por el administrador e indicada por el responsable.	

SEGURIDAD LÓGICA	
REVISIÓN PERIÓDICA DE USUARIOS	
PREGUNTA 34	
El administrador (o personal encargado de administrar los accesos) actualiza en el servidor (sistema operativo) "Y" con las indicaciones recibidas del responsable funcional.	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable mantener una segregación de funciones que se encarguen de revisar los usuarios y proceder a realizar las acciones necesarias.
COMENTARIOS	
Según la sección 404 de SOX es recomendable realizar una revisión periódica de usuarios de cada sistema operativo, ejecutada por el administrador e indicada por el responsable.	

SEGURIDAD LÓGICA	
ALTOS PRIVILEGIOS DE USUARIOS	
PREGUNTA 35	
Los usuarios con altos privilegios se encuentran asignados en la aplicación de forma razonable y coherente de acuerdo a las funciones en el servidor (sistema operativo) “Y”.	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable que los usuarios con altos privilegios se encuentren correctamente asignados a los usuarios.
COMENTARIOS	
Según la sección 404 de SOX es recomendable limitar los usuarios con altos privilegios al menor número de personas dado que mantienen la posibilidad de ejecutar transacciones críticas en los sistemas operativos.	

SEGURIDAD LÓGICA	
ALTOS PRIVILEGIOS DE USUARIOS	
PREGUNTA 36	
Verificar que el personal encargado de la administración de usuarios en el servidor (sistema operativo) “Y” no tiene acceso a transacciones incompatibles con sus funciones o innecesarias para la labor que realizan.	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable que los usuarios con altos privilegios se encuentren correctamente segregados de la ejecución de acciones con incidencia contable.
COMENTARIOS	
Según la sección 404 de SOX es recomendable que exista una correcta segregación de funciones entre la administración y la ejecución de transacciones de operación del sistema operativo.	

SEGURIDAD LÓGICA	
CUENTAS GENÉRICAS DE USUARIO	
PREGUNTA 37	
Las cuentas genéricas, en caso de existir, pertenecen a cuentas por defecto del servidor (sistema operativo) "Y" o se encuentran debidamente justificadas.	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable mantener un control de las cuentas genéricas y de las funciones que se realizan con las mismas.
COMENTARIOS	
Según la sección 404 de SOX es recomendable que las cuentas genéricas se encuentren controladas en los sistemas operativos.	

SEGURIDAD LÓGICA	
PISTAS DE AUDITORÍA	
PREGUNTA 38	
El responsable funcional ha determinado qué evento tiene impacto en la información financiera (evento crítico) y se va a recoger dentro de la pista de auditoría del servidor (sistema operativo) "Y".	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 39
Respuesta 2	No -> Es recomendable definir los eventos considerados críticos en el sistema operativo.
COMENTARIOS	
Según la sección 404 de SOX es recomendable registrar en los sistemas operativos los eventos críticos que puedan repercutir contablemente de algún modo.	

SEGURIDAD LÓGICA	
PISTAS DE AUDITORÍA	
PREGUNTA 39	
Se han activado por la gerencia de seguridad informática (o personal encargado) las pistas de auditoría con las información financiera crítica solicitada por el responsable funcional en el servidor (sistema operativo) “Y”.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 40
Respuesta 2	No -> Es recomendable activar las trazas de auditoría con la información financiera crítica.
COMENTARIOS	
Según la sección 404 de SOX es recomendable registrar en los sistemas operativos los eventos críticos que puedan repercutir contablemente de algún modo.	

SEGURIDAD LÓGICA	
PISTAS DE AUDITORÍA	
PREGUNTA 40	
En la pista de auditoría se registra: fecha, nombre del usuario que ejecutó el proceso y el evento registrado para el servidor (sistema operativo) “Y”.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 41
Respuesta 2	No -> Es recomendable almacenar la información necesaria para identificar los eventos.
COMENTARIOS	
Según la sección 404 de SOX es recomendable registrar en los sistemas operativos los eventos críticos que puedan repercutir contablemente de algún modo.	

SEGURIDAD LÓGICA	
PISTAS DE AUDITORÍA	
PREGUNTA 41	
El responsable funcional (o personas en las que delega) revisa periódicamente el listado de pistas de auditoría del servidor (sistema operativo) "Y". Este atributo no aplica en aquellos casos en los cuales el log es revisado tras la ocurrencia de un incidente (como control de detección).	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable revisar y mantener un control de los listados de auditoría registrados en el sistema operativo.
COMENTARIOS	
Según la sección 404 de SOX es recomendable revisar los eventos críticos de los sistemas operativos que puedan repercutir contablemente de algún modo.	

SEGURIDAD LÓGICA	
CONTROL DE ACCESOS	
PREGUNTA 42	
Existencia de un procedimiento de gestión de usuarios a nivel de base de datos que describa las distintas etapas del proceso así como las personas responsables.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 43
Respuesta 2	No -> Es recomendable que exista un procedimiento a nivel de base de datos que recoja el detalle del proceso y las personas responsables de cada etapa.
COMENTARIOS	
Según la sección 404 de SOX es recomendable mantener un procedimiento formalizado que recoja el detalle del proceso de gestión a nivel de base de datos que será utilizado en el momento de ejecutar las solicitudes.	

SEGURIDAD LÓGICA	
CONTROL DE ACCESOS	
PREGUNTA 43	
Existencia de una solicitud documentada de alta, baja o modificación de usuario de la base de datos “Z”.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 44
Respuesta 2	No -> Es recomendable que exista una petición que recoja los datos de los usuarios así como los permisos que se solicitan en la base de datos.
COMENTARIOS	
Según la sección 404 de SOX es recomendable mantener un control de gestión de los usuarios con acceso a las bases de datos.	

SEGURIDAD LÓGICA	
CONTROL DE ACCESOS	
PREGUNTA 44	
La petición del usuario de la base de datos “Z” se encuentra revisada y aprobada por el responsable funcional.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 45
Respuesta 2	No -> Es recomendable que la petición además de existir se encuentra revisada y aprobada por el responsable funcional.
COMENTARIOS	
Según la sección 404 de SOX es recomendable mantener un control de gestión de los usuarios con acceso a las bases de datos.	

SEGURIDAD LÓGICA	
CONTROL DE ACCESOS	
PREGUNTA 45	
En caso de alta/modificación: el nivel de autorización especificado en la solicitud de acceso coincide con la autorización asignada en la base de datos "Z".	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 46
Respuesta 2	No -> Es recomendable este autorizada por el responsable funcional autorizado en la base de datos.
COMENTARIOS	
Según la sección 404 de SOX es recomendable mantener un control de gestión de los usuarios con acceso a las bases de datos.	

SEGURIDAD LÓGICA	
CONTROL DE ACCESOS	
PREGUNTA 46	
En caso de alta/modificación: El acceso concedido en la base de datos "Z" se corresponde con las funciones del usuario	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable que el usuario dado de alta/modificado cuente con el permiso acorde a sus funciones.
COMENTARIOS	
Según la sección 404 de SOX es recomendable mantener un control de gestión de los usuarios con acceso a las bases de datos.	

SEGURIDAD LÓGICA	
CONTROL DE ACCESOS	
PREGUNTA 47	
En caso de baja: el usuario no tiene acceso a la base de datos (deshabilitado o eliminado) "Z".	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable dar de baja o deshabilitar el usuario en tiempo y forma en la base de datos.
COMENTARIOS	
Según la sección 404 de SOX es recomendable mantener un control de gestión de los usuarios con acceso a las bases de datos.	

SEGURIDAD LÓGICA	
CALIDAD DE LAS CONTRASEÑAS	
PREGUNTA 48	
Analizar la forma en que se crean y asignan las contraseñas para los usuarios de la base de datos "Z" y comprobar si es adecuada a) solicitud de cambio en el primer acceso b) longitud mínima c) caducidad de las contraseñas d) número de intentos fallidos antes de bloqueo	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable definir los parámetros de forma razonable y adecuada.
COMENTARIOS	
Según la sección 404 de SOX es recomendable mantener una configuración de seguridad adecuada en la base de datos.	

SEGURIDAD LÓGICA	
REVISIÓN PERIÓDICA DE USUARIOS	
PREGUNTA 49	
El administrador (o personal encargado de administrar los accesos) envía al responsable funcional un listado con las cuentas activas en el sistema y sus perfiles asociados en la base de datos “Z”.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 50
Respuesta 2	No -> Es recomendable mantener una segregación de funciones que se encarguen de revisar los usuarios y proceder a realizar las acciones necesarias.
COMENTARIOS	
Según la sección 404 de SOX es recomendable realizar una revisión periódica de usuarios de cada base de datos, ejecutada por el administrador e indicada por el responsable.	

SEGURIDAD LÓGICA	
REVISIÓN PERIÓDICA DE USUARIOS	
PREGUNTA 51	
El responsable funcional analiza los usuarios dados de alta así como la adecuación de los perfiles configurados en la base de datos “Z”.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 52
Respuesta 2	No -> Es recomendable mantener una segregación de funciones que se encarguen de revisar los usuarios y proceder a realizar las acciones necesarias.
COMENTARIOS	
Según la sección 404 de SOX es recomendable realizar una revisión periódica de usuarios de cada base de datos, ejecutada por el administrador e indicada por el responsable.	

SEGURIDAD LÓGICA	
REVISIÓN PERIÓDICA DE USUARIOS	
PREGUNTA 52	
Una vez revisado el listado, el responsable funcional responde al administrador (o personal encargado de administrar los accesos) validando los usuarios o indicando las modificaciones necesarias para la base de datos “Z”.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 53
Respuesta 2	No -> Es recomendable mantener una segregación de funciones que se encarguen de revisar los usuarios y proceder a realizar las acciones necesarias.
COMENTARIOS	
Según la sección 404 de SOX es recomendable realizar una revisión periódica de usuarios de cada base de datos, ejecutada por el administrador e indicada por el responsable.	

SEGURIDAD LÓGICA	
REVISIÓN PERIÓDICA DE USUARIOS	
PREGUNTA 53	
El administrador (o personal encargado de administrar los accesos) actualiza en la base de datos “Z” con las indicaciones recibidas del responsable funcional.	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable mantener una segregación de funciones que se encarguen de revisar los usuarios y proceder a realizar las acciones necesarias.
COMENTARIOS	
Según la sección 404 de SOX es recomendable realizar una revisión periódica de usuarios de cada base de datos, ejecutada por el administrador e indicada por el responsable.	

SEGURIDAD LÓGICA	
ALTOS PRIVILEGIOS DE USUARIOS	
PREGUNTA 54	
Los usuarios con altos privilegios se encuentran asignados en la aplicación de forma razonable y coherente de acuerdo a las funciones en la base de datos “Z”.	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable que los usuarios con altos privilegios se encuentren correctamente asignados a los usuarios.
COMENTARIOS	
Según la sección 404 de SOX es recomendable limitar los usuarios con altos privilegios al menor número de personas dado que mantienen la posibilidad de ejecutar transacciones críticas en las bases de datos.	

SEGURIDAD LÓGICA	
ALTOS PRIVILEGIOS DE USUARIOS	
PREGUNTA 55	
Verificar que el personal encargado de la administración de usuarios en la base de datos “Z” no tiene acceso a transacciones incompatibles con sus funciones o innecesarias para la labor que realizan.	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable que los usuarios con altos privilegios se encuentren correctamente segregados de la ejecución de acciones con incidencia contable.
COMENTARIOS	
Según la sección 404 de SOX es recomendable que exista una correcta segregación de funciones entre la administración y la ejecución de transacciones de operación de la base de datos..	

SEGURIDAD LÓGICA	
CUENTAS GENÉRICAS DE USUARIO	
PREGUNTA 56	
Las cuentas genéricas, en caso de existir, pertenecen a cuentas por defecto de la base de datos “Z” o se encuentran debidamente justificadas.	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable mantener un control de las cuentas genéricas y de las funciones que se realizan con las mismas.
COMENTARIOS	
Según la sección 404 de SOX es recomendable que las cuentas genéricas se encuentren controladas en las bases de datos.	

SEGURIDAD LÓGICA	
PISTAS DE AUDITORÍA	
PREGUNTA 57	
El responsable funcional ha determinado qué evento tiene impacto en la información financiera (evento crítico) y se va a recoger dentro de la pista de auditoría de la base de datos “Z”.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 58
Respuesta 2	No -> Es recomendable definir los eventos considerados críticos en la aplicación.
COMENTARIOS	
Según la sección 404 de SOX es recomendable registrar en las bases de datos los eventos críticos que puedan repercutir contablemente de algún modo.	

SEGURIDAD LÓGICA	
PISTAS DE AUDITORÍA	
PREGUNTA 58	
Se han activado por la gerencia de seguridad informática (o personal encargado) las pistas de auditoría con las información financiera crítica solicitada por el responsable funcional en la base de datos “Z”.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 59
Respuesta 2	No -> Es recomendable activar las trazas de auditoría con la información financiera crítica.
COMENTARIOS	
Según la sección 404 de SOX es recomendable registrar en las bases de datos los eventos críticos que puedan repercutir contablemente de algún modo.	

SEGURIDAD LÓGICA	
PISTAS DE AUDITORÍA	
PREGUNTA 59	
En la pista de auditoría se registra: fecha, nombre del usuario que ejecutó el proceso y el evento registrado para la base de datos “Z”.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 60
Respuesta 2	No -> Es recomendable almacenar la información necesaria para identificar los eventos.
COMENTARIOS	
Según la sección 404 de SOX es recomendable registrar en las bases de datos los eventos críticos que puedan repercutir contablemente de algún modo.	

SEGURIDAD LÓGICA	
PISTAS DE AUDITORÍA	
PREGUNTA 61	
El responsable funcional (o personas en las que delega) revisa periódicamente el listado de pistas de auditoría de la base de datos "Z". Este atributo no aplica en aquellos casos en los cuales el log es revisado tras la ocurrencia de un incidente (como control de detección).	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable revisar y mantener un control de los listados de auditoría registrados en la aplicación.
COMENTARIOS	
Según la sección 404 de SOX es recomendable revisar los eventos críticos que puedan repercutir contablemente de algún modo.	

6.2 OPERACIONES – EXPLOTACIÓN DE SISTEMAS

Este grupo va a incluir controles y actividades que cubran objetivos como la copia de seguridad de información de los distintos sistemas, de forma que esta información se pueda recuperar si fuese necesario, procesos programados, la gestión de las incidencias relacionada con los sistemas o los cambios en infraestructuras, cambios en los procesos programados, etc.

OPERACIONES	
SALVAGUARDA DE INFORMACIÓN (BACKUP)	
PREGUNTA 62	
Existe un procedimiento para la gestión de las copias de seguridad y recuperación de datos donde se describe el proceso a seguir, personas responsables y periodicidad.	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Continuaremos con la pregunta 63. Es recomendable que exista un procedimiento para la gestión de las copias de seguridad y la recuperación de los datos.
COMENTARIOS	
Según la sección 404 de SOX es recomendable que se encuentre definido un procedimiento formal que recoja la información del proceso de copias de seguridad y recuperación de datos así como las personas responsables de cada una de las etapas.	

OPERACIONES	
SALVAGUARDA DE INFORMACIÓN (BACKUP)	
PREGUNTA 63	
La copia de seguridad recoge los datos de la aplicación y base de datos.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 64
Respuesta 2	No -> Es recomendable que la copia de seguridad almacene los datos de la aplicación y base de datos.
COMENTARIOS	
Según la sección 404 de SOX es recomendable que las copias de seguridad recojan la información de cada aplicación en el alcance de la auditoría.	

OPERACIONES	
SALVAGUARDA DE INFORMACIÓN (BACKUP)	
PREGUNTA 64	
El proceso copia de seguridad ha finalizado correctamente, verificando que el soporte de copia superó su vida útil. En caso de error, éste queda registrado, se analiza el motivo y se corrige.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 65
Respuesta 2	No -> Es recomendable que los procesos de seguridad finalicen correctamente.
COMENTARIOS	
Según la sección 404 de SOX es recomendable que se mantenga un control de la ejecución del proceso de copia de forma que se verifique que finalizan correctamente.	

OPERACIONES	
SALVAGUARDA DE INFORMACIÓN (BACKUP)	
PREGUNTA 66	
La copia de seguridad está almacenada correctamente (lugar identificable y fácilmente ubicable).	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable que las copias se almacenen en un lugar seguro y con disponibilidad.
COMENTARIOS	
Según la sección 404 de SOX es recomendable que las copias de seguridad se encuentren accesibles y disponibles.	

OPERACIONES	
TAREAS PROGRAMADAS	
PREGUNTA 67	
Existe un procedimiento para la gestión de tareas programadas donde se describe el proceso a seguir, personas responsables y periodicidad.	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Continuaremos con la pregunta 68. Es recomendable que exista un procedimiento para la gestión de las tareas programadas.
COMENTARIOS	
Según la sección 404 de SOX es recomendable que se encuentre definido un procedimiento formal que recoja la información del proceso de tareas programadas así como las personas responsables de cada una de las etapas.	

OPERACIONES	
TAREAS PROGRAMADAS	
PREGUNTA 68	
Existe una solicitud de planificación de tarea.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 69
Respuesta 2	No -> Es recomendable que se solicite la planificación de la tarea y quede un registro de la solicitud.
COMENTARIOS	
Según la sección 404 de SOX es recomendable que la planificación de las tareas programadas sea solicitada y registrada debidamente.	

OPERACIONES	
TAREAS PROGRAMADAS	
PREGUNTA 69	
Existe una autorización para la ejecución de la tarea programada.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 70
Respuesta 2	No -> Es recomendable que la solicitud se encuentre autorizada por un responsable.
COMENTARIOS	
Según la sección 404 de SOX es recomendable que las solicitudes, además de existir, se encuentren autorizadas por un responsable.	

OPERACIONES	
TAREAS PROGRAMADAS	
PREGUNTA 70	
La tarea planificada ha terminado correctamente. En caso de haberse producido una ejecución incorrecta de la tarea planificada, acciones tomadas para la solución del error.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 71
Respuesta 2	No -> Es recomendable la verificación de que la tarea ha finalizado correctamente.
COMENTARIOS	
Según la sección 404 de SOX es recomendable que exista un control que verifique que las tareas finalizan correctamente, y en caso de producirse un error este es subsanado adecuadamente.	

OPERACIONES	
TAREAS PROGRAMADAS	
PREGUNTA 71	
Existe una adecuada segregación de funciones entre los responsables de la gestión de las tareas programadas.	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable que el personal que tienen la posibilidad de realizar solicitudes se encuentren diferenciadas del personal autorizador y del personal de desarrollo que tiene la posibilidad de planificar las tareas.
COMENTARIOS	
Según la sección 404 de SOX es recomendable que exista una correcta segregación de funciones en el proceso de gestión de las tareas programadas.	

OPERACIONES	
GESTIÓN DE INCIDENCIAS	
PREGUNTA 72	
Existe un procedimiento para la gestión de las incidencias donde se describe el proceso a seguir, personas responsables, herramienta utilizada y detalle acerca de la prioridad.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 73
Respuesta 2	No -> Es recomendable que exista un procedimiento para la gestión de las incidencias.
COMENTARIOS	
Según la sección 404 de SOX es recomendable que se encuentre definido un procedimiento formal que recoja la información del proceso de las incidencias así como las personas responsables de cada una de las etapas.	

OPERACIONES	
GESTIÓN DE INCIDENCIAS	
PREGUNTA 73	
Existencia de solicitud de apertura de incidencia, verificando que se pueden identificar la aplicación/plataforma afectada por la incidencia	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 74
Respuesta 2	No -> Es recomendable que exista una solicitud de apertura de la incidencia que contenga los detalles de la misma y la aplicación afectada.
COMENTARIOS	
Según la sección 404 de SOX es recomendable que se registren las incidencias relacionadas con cada aplicación.	

OPERACIONES	
GESTIÓN DE INCIDENCIAS	
PREGUNTA 74	
La incidencia está clasificada por su prioridad (alta, baja, grave, media, absoluta, etc.)	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 75
Respuesta 2	No -> Es recomendable que exista una solicitud de apertura de la incidencia que contenga los detalles de la misma.
COMENTARIOS	
Según la sección 404 de SOX es recomendable que se registren las incidencias indicando su prioridad según la criticidad.	

OPERACIONES	
GESTIÓN DE INCIDENCIAS	
PREGUNTA 75	
La incidencia ha sido resuelta, indicando las medidas realizadas para solventarla, quien ha realizado las acciones para solventarla, fecha de realización de dichas acciones.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 76
Respuesta 2	No -> Es recomendable que las incidencias sean resueltas en tiempo y forma indicando los detalles de resolución.
COMENTARIOS	
Según la sección 404 de SOX es recomendable que se registren las incidencias desde su apertura hasta su resolución.	

OPERACIONES	
GESTIÓN DE INCIDENCIAS	
PREGUNTA 76	
La resolución de la incidencia ha sido comunicada al usuario que la originó.	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable que el usuario sea informado de la resolución de la incidencia.
COMENTARIOS	
Según la sección 404 de SOX es recomendable que se realice la comunicación debida a los usuarios que originan las incidencias.	

OPERACIONES	
GESTIÓN DE INCIDENCIAS	
PREGUNTA 77	
Existencia de un proceso de monitorización de las incidencias abiertas.	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable que se realice un seguimiento de las incidencias abiertas indicando las acciones que se realizan para el cierre de las mismas.
COMENTARIOS	
Según la sección 404 de SOX es recomendable que exista un control de monitorización de las incidencias abiertas.	

OPERACIONES	
GESTÓN DE CAMBIOS EN INFRAESTRUCTURA	
PREGUNTA 78	
Existe un procedimiento para la gestión de los cambios en infraestructuras donde se describe el proceso a seguir y personas responsables.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 79
Respuesta 2	No -> Es recomendable que exista un procedimiento para la gestión de cambios en infraestructuras.
COMENTARIOS	
Según la sección 404 de SOX es recomendable que se encuentre definido un procedimiento formal que recoja la información del proceso de cambios en infraestructuras así como las personas responsables de cada una de las etapas.	

OPERACIONES	
GESTIÓN DE CAMBIOS EN INFRAESTRUCTURA	
PREGUNTA 79	
Existe una solicitud que describe la naturaleza (sistema afectado), prioridad y la justificación del cambio.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 80
Respuesta 2	No -> Es recomendable que exista una solicitud que describa el detalle del cambio.
COMENTARIOS	
Según la sección 404 de SOX es recomendable que registren el detalle de las solicitudes de los cambios realizados en los sistemas.	

OPERACIONES	
GESTIÓN DE CAMBIOS EN INFRAESTRUCTURA	
PREGUNTA 80	
El cambio ha sido probado en un entorno de pruebas/certificación (pre-producción).	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 81
Respuesta 2	No -> Es recomendable que el cambio se probado antes de implantarlo en producción.
COMENTARIOS	
Según la sección 404 de SOX es recomendable que se realicen pruebas en un entorno segregado antes de su puesta en producción.	

OPERACIONES	
GESTIÓN DE CAMBIOS EN INFRAESTRUCTURA	
PREGUNTA 81	
El responsable correspondiente ha autorizado implementación en producción del cambio solicitado.	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable que los cambios sean autorizados por el responsable antes de su puesta en producción.
COMENTARIOS	
Según la sección 404 de SOX es recomendable que exista un control en el que se autorice el cambio antes de su puesta en producción.	

OPERACIONES	
GESTIÓN DE CAMBIOS EN INFRAESTRUCTURA	
PREGUNTA 82	
La puesta en producción ha sido realizada por el personal técnico adecuado.	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable que exista un personal segregado encargado de realizar las puestas en producción.
COMENTARIOS	
Según la sección 404 de SOX es recomendable que exista un personal segregado encargado de realizar las puestas en producción.	

6.3 DESARROLLO DE SISTEMAS - CAMBIOS A PROGRAMAS

El grupo relacionado con los cambios a programas incluye controles y actividades que cubran el ciclo de vida de los cambios, es decir, desde que se solicitan los mismos hasta que se ponen en producción. Controles que aseguren que los cambios están correctamente solicitados, debidamente autorizados, probados y puestos en producción entre otros.

DESARROLLO DE SISTEMAS	
GESTÓN DE CAMBIOS A PROGRAMAS	
PREGUNTA 83	
Existe un procedimiento para la gestión de los cambios o nuevo desarrollos en programas donde se describe el proceso a seguir y personas responsables.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 84
Respuesta 2	No -> Es recomendable que exista un procedimiento para la gestión de cambios en programas o nuevos desarrollos.
COMENTARIOS	
Según la sección 404 de SOX es recomendable que se encuentre definido un procedimiento formal que recoja la información del proceso de cambios en programas o nuevos desarrollos así como las personas responsables de cada una de las etapas.	

DESARROLLO DE SISTEMAS	
GESTIÓN DE CAMBIOS A PROGRAMAS	
PREGUNTA 84	
Existe una solicitud que describe la naturaleza (sistema afectado) y la extensión del cambio.	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 85
Respuesta 2	No -> Es recomendable que exista una solicitud que describa el detalle del cambio.
COMENTARIOS	
Según la sección 404 de SOX es recomendable que registren el detalle de las solicitudes de los cambios realizados en los programas.	

DESARROLLO DE SISTEMAS	
GESTIÓN DE CAMBIOS A PROGRAMAS	
PREGUNTA 85	
El cambio ha sido probado en un entorno de pruebas/certificación (pre-producción).	
VALORACIONES	
Respuesta 1	Si -> Continuaremos con la pregunta 86
Respuesta 2	No -> Es recomendable que el cambio se probado antes de implantarlo en producción.
COMENTARIOS	
Según la sección 404 de SOX es recomendable que se realicen pruebas en un entorno segregado antes de su puesta en producción.	

DESARROLLO DE SISTEMAS	
GESTIÓN DE CAMBIOS A PROGRAMAS	
PREGUNTA 86	
El responsable correspondiente ha autorizado implementación en producción del cambio solicitado.	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable que los cambios sean autorizados por el responsable antes de su puesta en producción.
COMENTARIOS	
Según la sección 404 de SOX es recomendable que exista un control en el que se autorice el cambio antes de su puesta en producción.	

DESARROLLO DE SISTEMAS	
GESTIÓN DE CAMBIOS A PROGRAMAS	
PREGUNTA 87	
La puesta en producción ha sido realizada por el personal técnico adecuado.	
VALORACIONES	
Respuesta 1	Si -> Satisfactorio
Respuesta 2	No -> Es recomendable que se realice un seguimiento de las incidencias abiertas indicando las acciones que se realizan para el cierre de las mismas.
COMENTARIOS	
Según la sección 404 de SOX es recomendable que exista un control de monitorización de las incidencias abiertas.	

6.4 VALORACIÓN DEL MARCO DE EVALUACIÓN

Ésta marco de evaluación definida evaluara el grado de control informático de una organización. Para ello se evaluarán las distintas preguntas y respuestas, ya que en algunos casos será valorado que se cumpla el proceso completo, dependiendo del cumplimiento de cada pregunta/proceso se determinará la confianza o no confianza en los sistemas de la organización.

Como parte del cuestionario de revisión del entorno general informático, se formularán determinadas sugerencias de mejora sobre el sistema de control interno informático y riesgos asociados. Vamos a separar cada uno de ellos por cada área:

1. Seguridad física
2. Seguridad lógica
3. Operaciones
4. Desarrollo de Programas

CAPÍTULO 7

APLICACIÓN PARA LA EVALUACIÓN DEL GRADO DE CONFIANZA DE LOS SISTEMAS DE LA INFORMACIÓN

7. APLICACIÓN PARA LA EVALUACIÓN DEL GRADO DE CONFIANZA DE LOS SISTEMAS DE INFORMACIÓN

7.1 OBJETIVOS DEL PROGRAMA

El objetivo principal de la aplicación creada es conocer el grado de confianza que ofrecen los sistemas que afectan a los estados financieros, mediante un análisis a través de una serie de preguntas acerca de la situación actual de los sistemas de la compañía.

7.2 ÁMBITO DE LA APLICACIÓN

Esta "auto-evaluación" tomará como base la ley Sarbanes-Oxley Act estudiada y analizada en este PFC, con la cual se detectan los sistemas en los que se puede depositar confianza por su correcta configuración y los que cuentan con alguna debilidad. Todo esto se determinará mediante una serie de cuestionarios que muestren su situación actual.

7.3 PUNTOS ANALIZABLES

Los puntos a analizar estarán relacionados con las siguientes áreas:

- ✓ Seguridad Física
- ✓ Seguridad Lógica
- ✓ Operaciones
- ✓ Cambios a programas

7.4 ¿PORQUÉ USARLO?

Esta sencilla aplicación aparte de ser una versión de software libre por el cuál no implica ningún tipo de gasto económico, consigue de una forma fácil, sencilla, rápida e intuitiva conocer cómo una compañía se encuentra en la actualidad con respecto a la confianza en sus sistemas, además de indicarte ciertas recomendaciones y consejos por los cuales puede realizar mejoras en los sistemas.

7.5 CAPTURAS DE LA APLICACIÓN

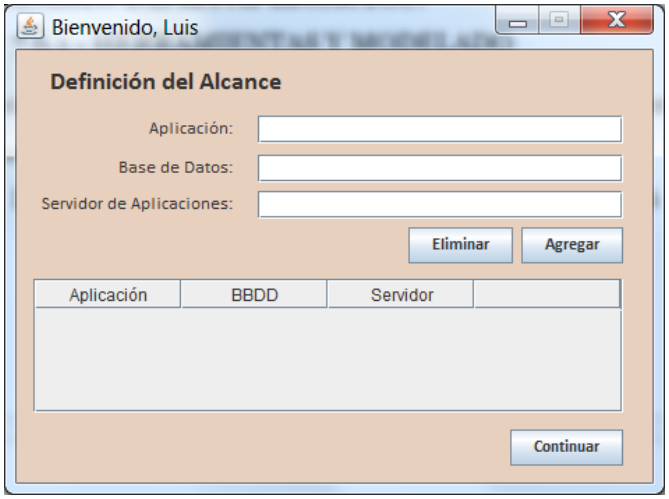


Figura 17. Menú inicial de introducción de sistemas

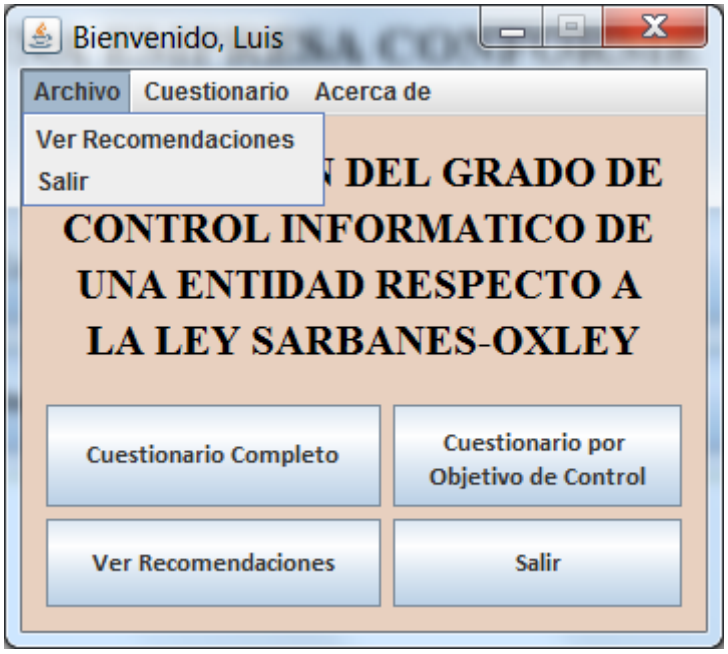


Figura 18. Menú principal

Figura 19. Menú cuestionario

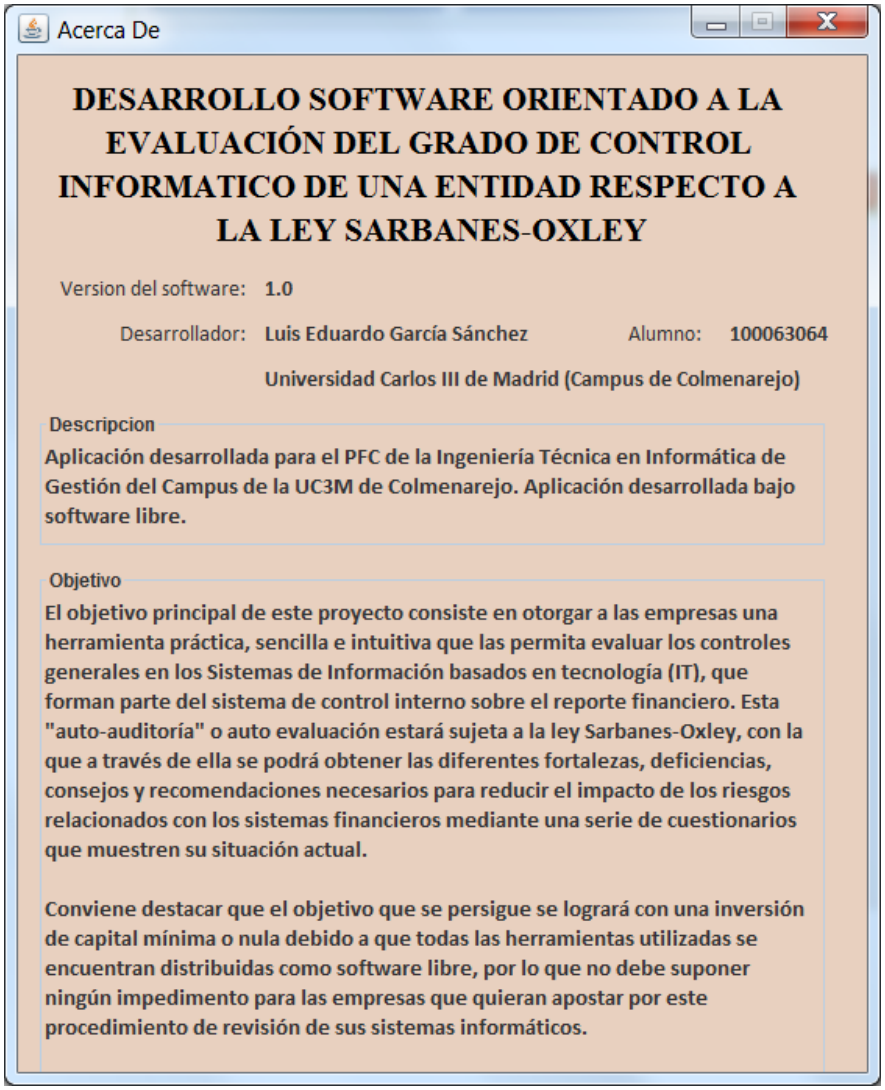


Figura 20. Menú Acerca de

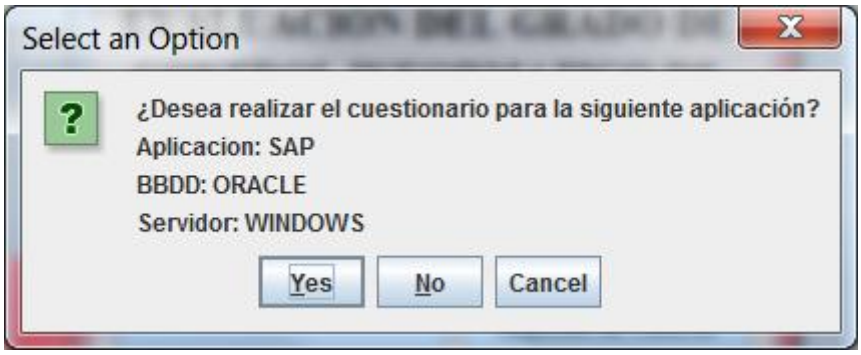


Figura 21. Menú de selección de la aplicación

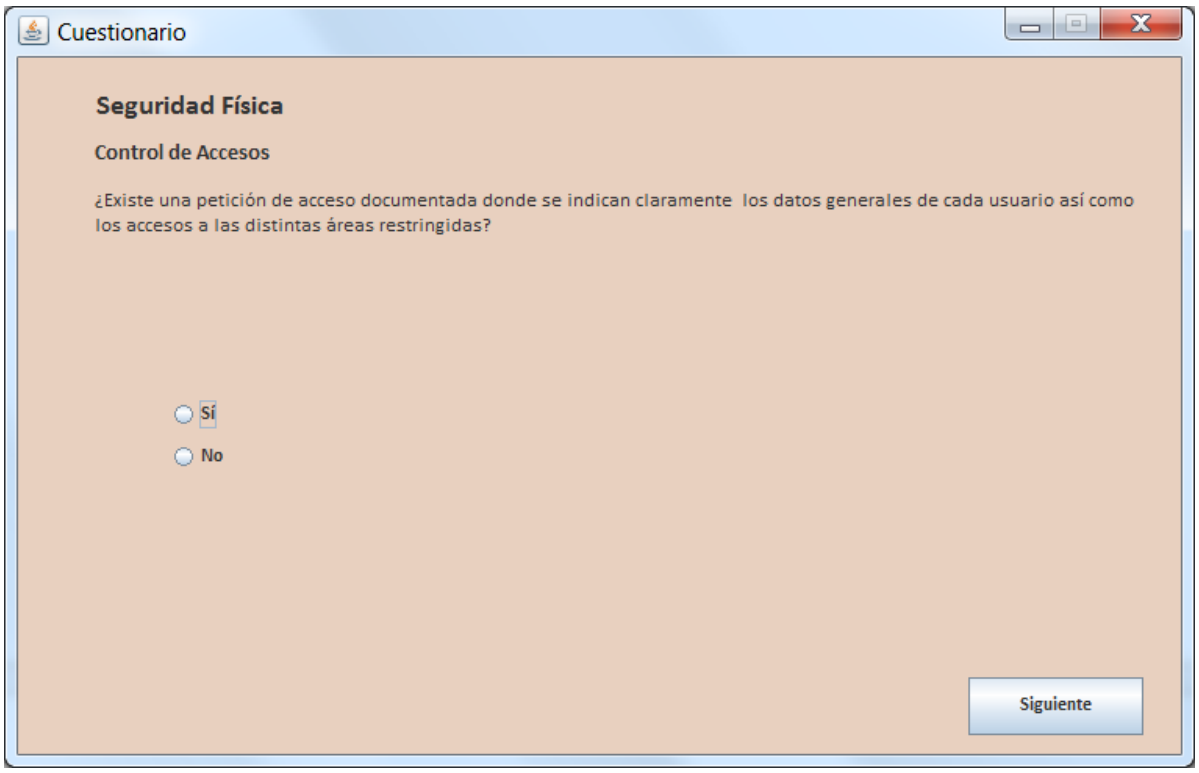


Figura 22. Ejemplo de pregunta de Seguridad física

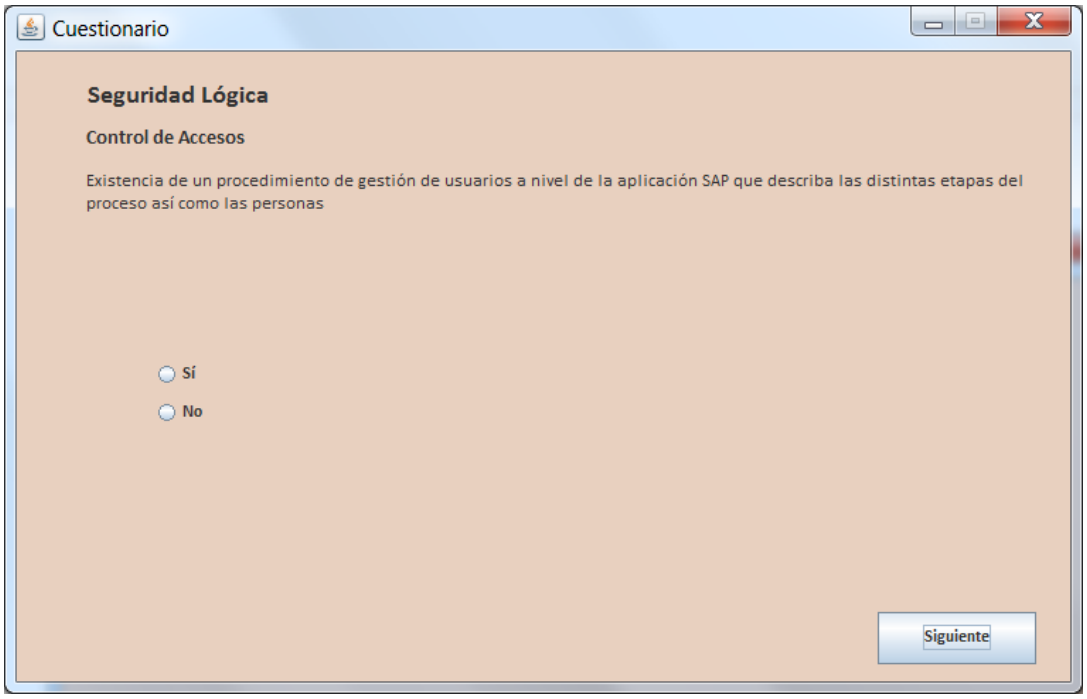


Figura 23. Ejemplo de pregunta de Seguridad lógica

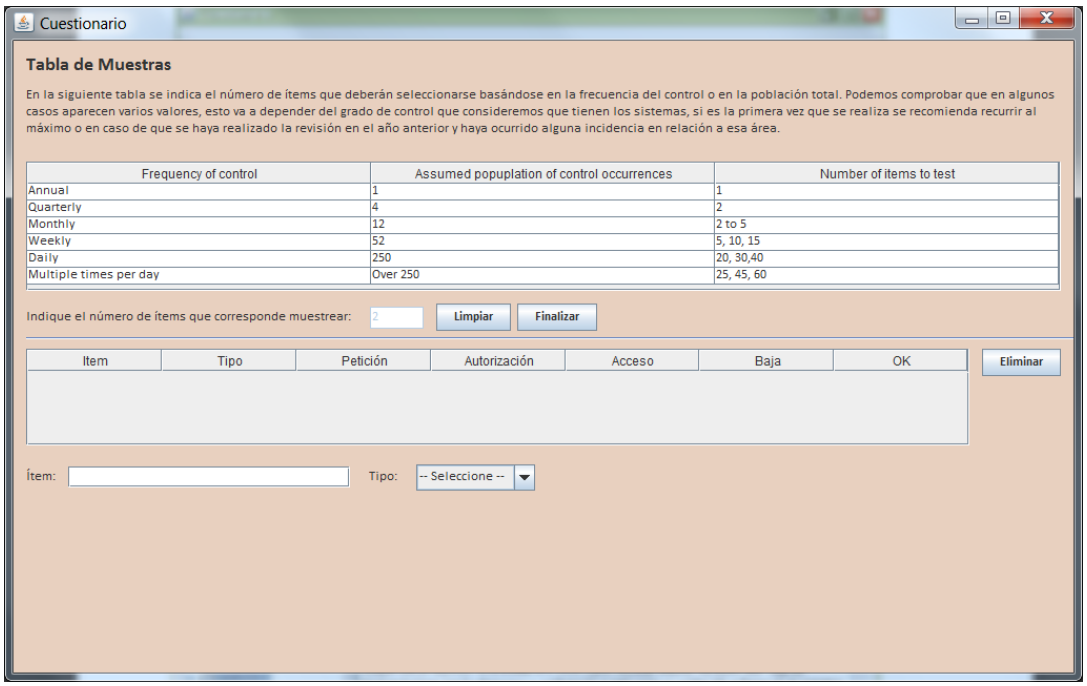


Figura 24. Pantalla de tabla de muestreo e introducción de ítems a testear

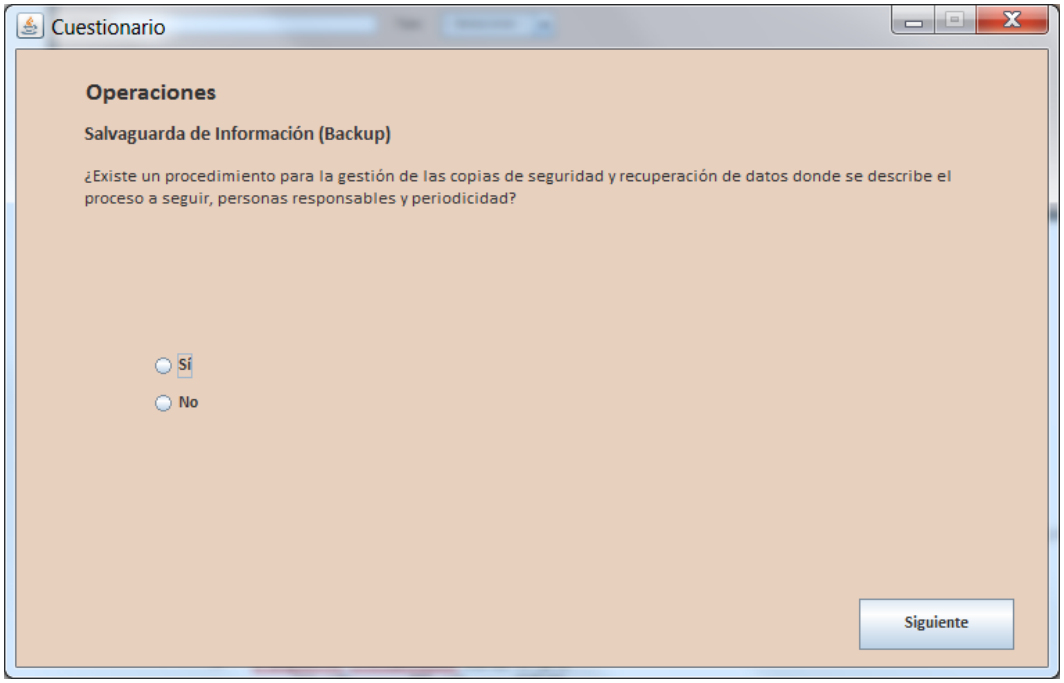


Figura 25. Ejemplo de pantalla de Operaciones

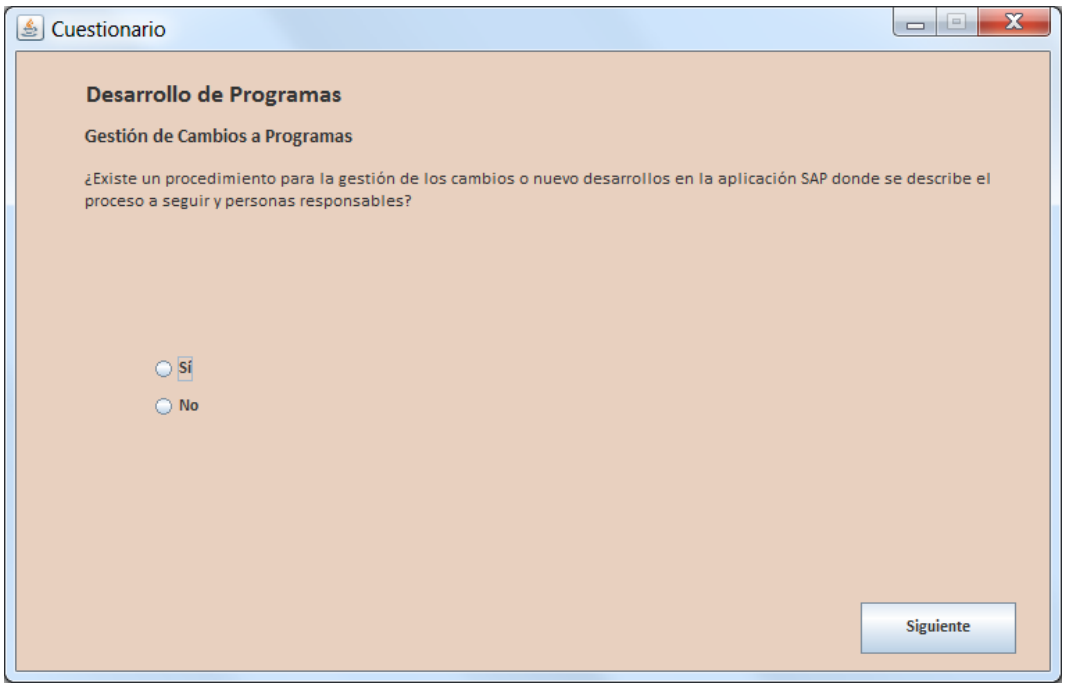


Figura 26. Ejemplo de pantalla de Desarrollo de Programas

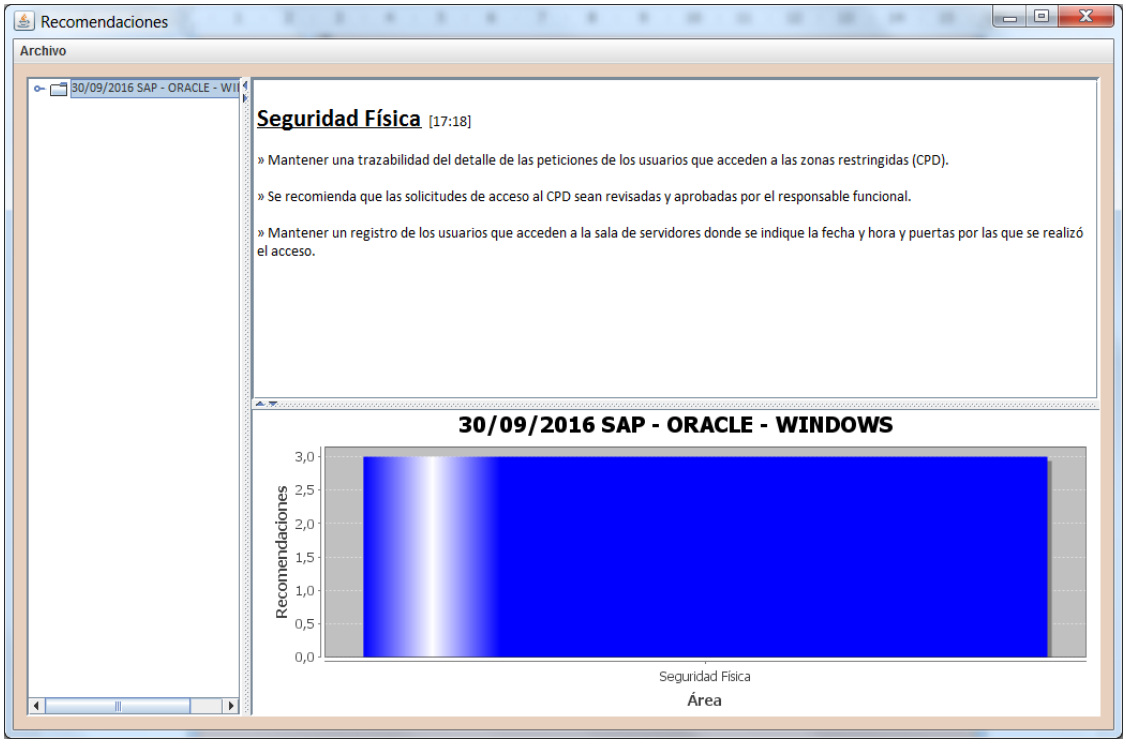


Figura 27. Pantalla del índice y detalle de recomendaciones

Figura 28. Consistencia en la BD

7.6 ANEXO DE LA APLICACIÓN

7.6.1 HERRAMIENTAS Y MODELADO

A continuación se enumerarán y detallaran las diferentes herramientas utilizadas en el desarrollo de esta aplicación software de auto-evaluación.

- Lenguaje de Programación Orientado a Objetos -> Java 6
  - Paquete NetBeans IDE 6.9.1
    - NetBeans Platform SDK
    - Java SE
    - JavaFX
    - Java Web y EE
    - Java ME
    - Java Card™ 3 Connected
    - Ruby C/C++
    - Groovy
    - PHP
    - Servidor GlassFish Server Open Source Edition 3.0.1
    - Servidor Apache Tomcat 6.0.26 [NETBEANS]

- Bases de Datos -> MySQL 5.1
  - Paquete XAMPP Windows 1.7.4
    - Servidor Apache 2.2.17
    - MySQL 5.5.8
    - PHP 5.3.5
    - phpMyAdmin 3.3.9
    - FileZilla FTP Server 0.9.37
    - Tomcat 7.0.3 (with mod_proxy_ajp as connector)

- Conector Base de Datos -> JDBC Driver for MySQL 5.1.16

Todas las aplicaciones de las que se hacen uso son de software libre, por lo que pueden descargarse de su página web oficial, en la que también se encontraran los diferentes requerimientos necesarios para su uso.

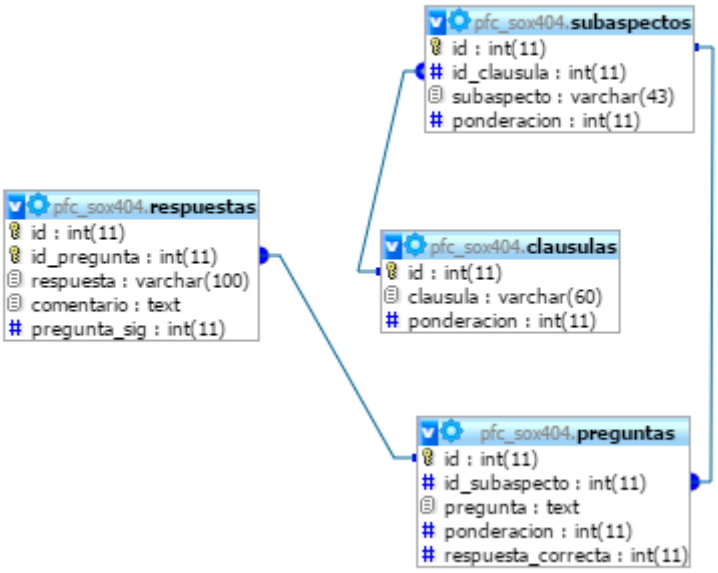


Figura 29. Tablas de referencias de la BD

CAPÍTULO 8

PLANIFICACIÓN Y PRESUPUESTO

8. PLANIFICACIÓN Y PRESUPUESTO

8.1 PLANIFICACIÓN

Dado el desarrollo realizado, se partió desde el inicio de una planificación con el fin de llevar a cabo un seguimiento durante todo el tiempo transcurrido en su elaboración. Para plasmar el mismo se ha utilizado un diagrama de Gantt que ver reflejado a continuación en distintos formatos.

	Modo de	Nombre de tarea	Duración	Comienzo	Fin
1		**Reuniones con tutor**	**223 días**	**lun 09/03/15**	**mié 13/01/16**
2		Reunión 1	1 día	lun 09/03/15	lun 09/03/15
3		Reunión 2	1 día	lun 13/04/15	lun 13/04/15
4		Reunión 3	1 día	lun 18/05/15	lun 18/05/15
5		Reunión 4	1 día	lun 22/06/15	lun 22/06/15
6		Reunión 5	1 día	lun 21/09/15	lun 21/09/15
7		Reunión 6	1 día	lun 19/10/15	lun 19/10/15
8		Reunión 7	1 día	lun 23/11/15	lun 23/11/15
9		Reunión 8	1 día	lun 14/12/15	lun 14/12/15
10		Reunión 9	1 día	mié 13/01/16	mié 13/01/16
11		**Fase de análisis**	**39 días**	**lun 09/03/15**	**jue 30/04/15**
12		Propuesta del proyecto	1 día	lun 09/03/15	lun 09/03/15
13		Estudios preliminares	30 días	mar 10/03/15	lun 20/04/15
14		Estudio previo de la BBDD	7 días	mar 21/04/15	mié 29/04/15
15		Resolución de incidencias y fin de la fase de análisis	1 día	jue 30/04/15	jue 30/04/15
16		**Fase de diseño**	**76 días**	**lun 04/05/15**	**lun 17/08/15**
17		Diseño de la interfaz gráfica	30 días	lun 04/05/15	vie 12/06/15
18		Diseño de la aplicación	45 días	lun 15/06/15	vie 14/08/15
19		Resolución de incidencias y fin de la fase de diseño	1 día	lun 17/08/15	lun 17/08/15
20		**Fase de implementación**	**67 días**	**mar 01/09/15**	**mié 02/12/15**
21		Implementación de la BBDD	15 días	mar 01/09/15	lun 21/09/15
22		Implementación de la aplicación	45 días	mar 22/09/15	lun 23/11/15
23		Resolución de incidencias y fin de la fase de implementación	7 días	mar 24/11/15	mié 02/12/15
24		Documentación	30 días	jue 03/12/15	mié 13/01/16
25		Fin de proyecto	2 días	jue 14/01/16	vie 15/01/16

Figura 30. Tareas del diagrama de Gantt

Como se muestra, desde el comiendo se ha dedicado un gran porcentaje de este tiempo a la documentación desde la toma de requisitos, conocimientos básicos, recopilación de conocimientos acerca de la implementación en las tecnologías hasta la redacción de la correspondiente memoria.

Además, se detallan las reuniones presenciales con el tutor dado que se incluye en estos tiempos las comunicaciones que se han ido realizando a través de medios electrónicos.

Por último, es importante mencionar que la tarea que mayor tiempo ha supuesto ha sido la correspondiente a la implementación.

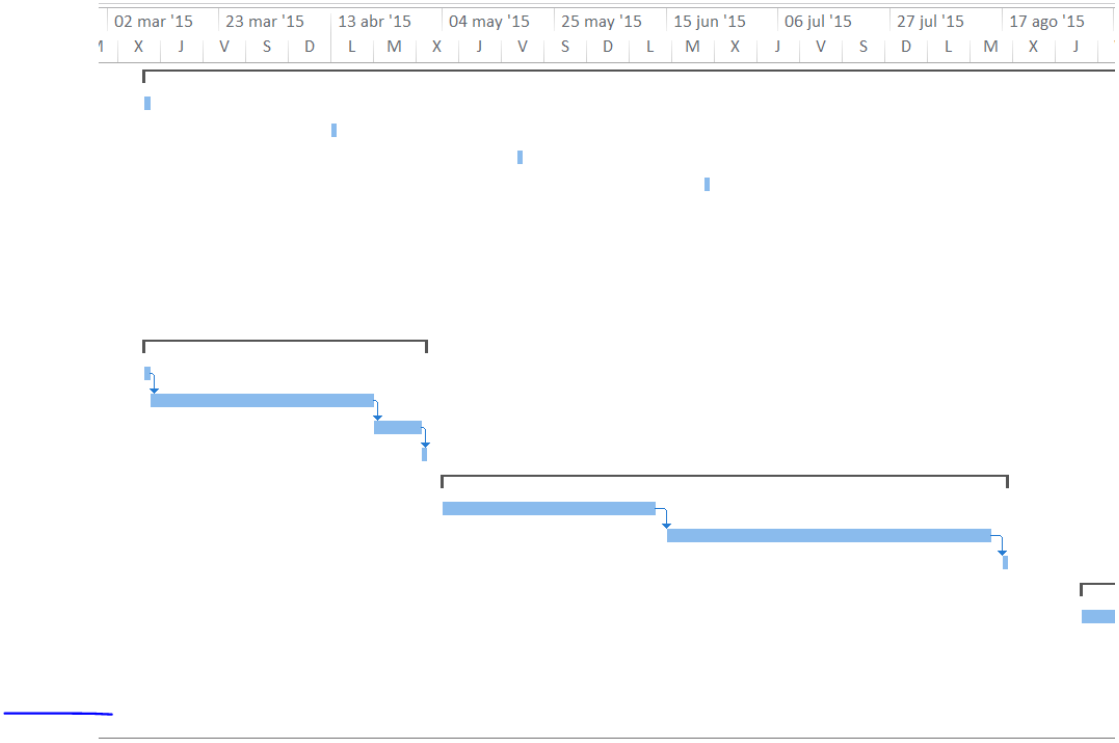


Figura 31. Diagrama de Gantt parte 1

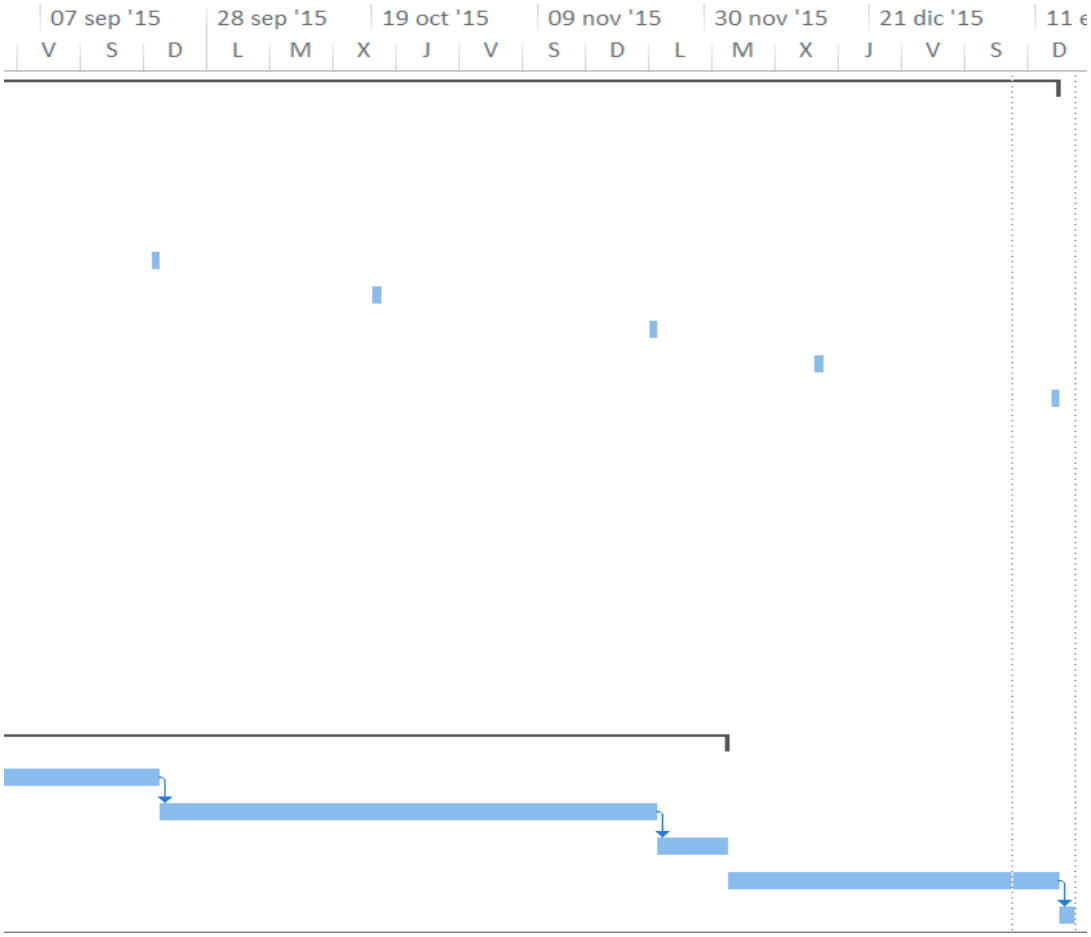


Figura 32. Diagrama de Gantt parte 2

8.2 PRESUPUESTO

A continuación, se muestra el presupuesto del proyecto, especificando los distintos gastos.

Para este desglose se tomará como base la plantilla sobre el presupuesto preparado proporcionado por la Universidad Carlos III de Madrid. Se va a proceder a separar los distintos aspectos que se muestran en el presupuesto:

Coste de personal imputable al proyecto

Partiendo de la duración del proyecto y el coste mensual que se indica en dicha plantilla se ha conseguido el siguiente coste, teniendo en cuenta la posición de Ingeniero:

Categoría	Dedicación (hombres mes)	Coste hombre mes	Coste (Euro)
Ingeniero	9	131,25 €	1.181,25 €

Tabla 3. Coste por personal

Coste de equipos, software y licencias

Para el correspondiente desarrollo del proyecto se han utilizado diferentes herramientas tanto para generar tanto el código de la aplicación como toda la documentación. Es importante mencionar que las aplicaciones utilizadas para la generación del código no han supuesto ningún coste dado. Por el contrario, para la creación de la planificación y documentación se han utilizado tanto un equipo como alguna herramienta del paquete Office, es por ello que se incluyen dichas licencias dentro del presupuesto.

La necesidad de disponer un equipo para llevar a cabo el desarrollo de un proyecto es necesaria y se han realizado algunas inversiones cuyos costes imputables se detallan a continuación. Cada uno de estos cálculos se ha realizado siguiendo la plantilla de presupuesto indicada anteriormente.

Descripción	Coste (Euro)	% Uso dedicado proyecto	Dedicación (meses)	Periodo de depreciación	Coste imputable [d)]
Pórtatil de trabajo	450,00	100	9	60	67,50
Microsoft Office 2007 Professional	290,00	10	1	60	0,48
Microsoft Office Project 2007	120,00	5	0,2	60	0,02
				Total	68,00

[d)] Fórmula de cálculo de la Amortización:

A = nº de meses desde la fecha de facturación en que el equipo es utilizado

B = periodo de depreciación (60 meses)

C = coste del equipo (sin IVA)

D = % del uso que se dedica al proyecto (habitualmente 100%)

Tabla 4. Coste de equipos, software y licencias

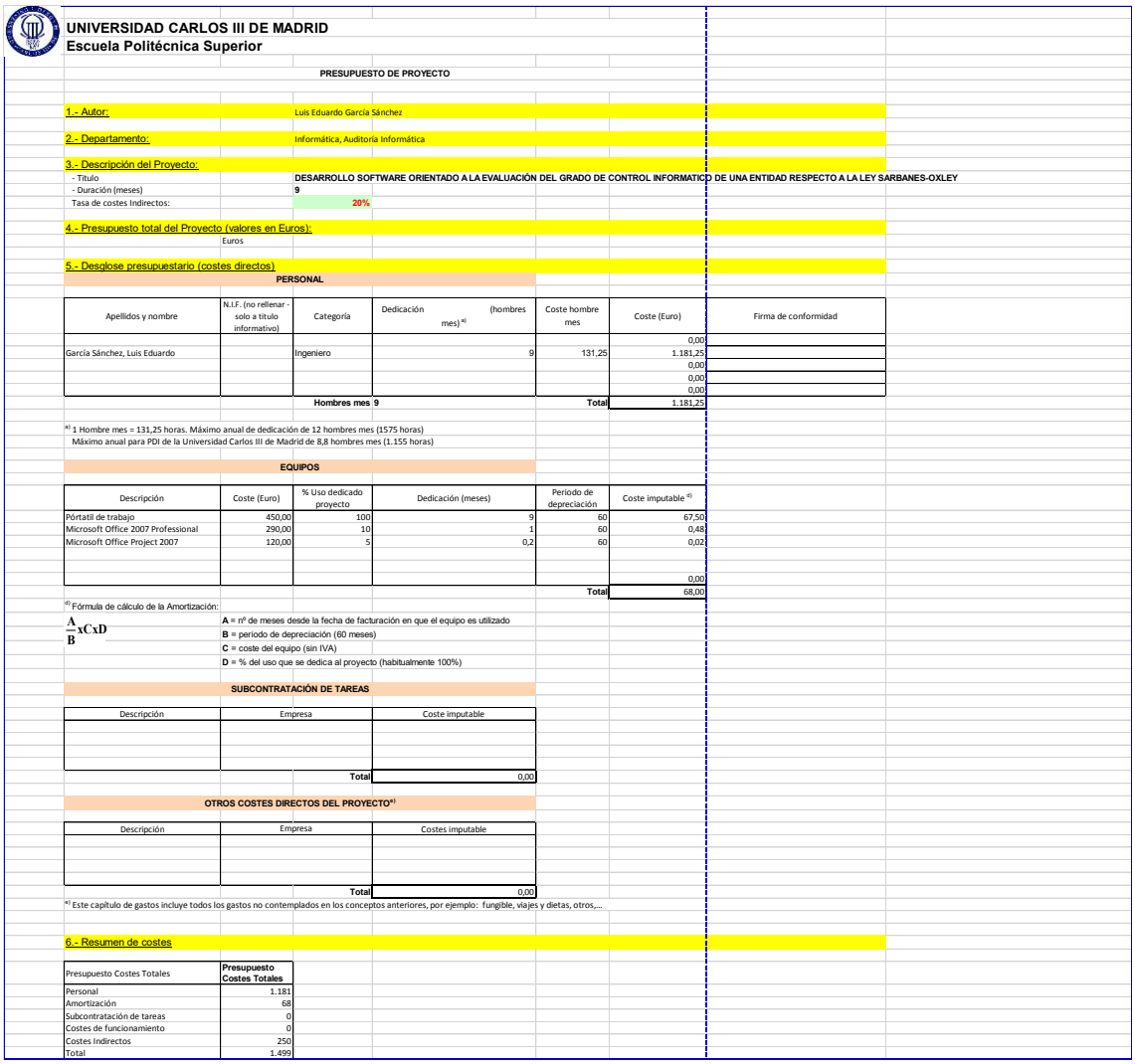
Resumen de costes

Para finalizar, indicaremos en la siguiente tabla el resumen de los costes mencionados anteriormente incluyendo una tasa de costes indirectos del 20% que será el presupuesto final alcanzado mediante el uso de la plantilla del presupuesto.

Presupuesto Costes Totales	Presupuesto Costes Totales
Personal	1.181,25 €
Amortización	68,00 €
Subcontratación de tareas	- €
Costes de funcionamiento	- €
Costes Indirectos	249,85 €
Total	1.499,10 €

Tabla 5. Resumen de costes

Plantilla de presupuesto



UNIVERSIDAD CARLOS III DE MADRID
Escuela Politécnica Superior

PRESUPUESTO DE PROYECTO

1.- Autor: Luis Eduardo García Sánchez

2.- Departamento: Informática, Auditoría Informática

3.- Descripción del Proyecto:
- Título: DESARROLLO SOFTWARE ORIENTADO A LA EVALUACIÓN DEL GRADO DE CONTROL INFORMATICO DE UNA ENTIDAD RESPECTO A LA LEY SARBANES-OXLEY
- Duración (meses): 9
Tasa de costes Indirectos: 20%

4.- Presupuesto total del Proyecto (valores en Euros): Euros

5.- Desglose presupuestario (costes directos)

PERSONAL

Apellidos y nombre	N.I.F. (no rellenar - solo a título informativo)	Categoría	Dedicación (hombres mes) [a]	Coste hombre mes	Coste (Euro)	Firma de conformidad
					0,00	
García Sánchez, Luis Eduardo		Ingeniero	9	131,25	1.181,25	
					0,00	
					0,00	
					0,00	
		Hombres mes	9	Total	1.181,25	

[a] 1 Hombre mes = 131,25 horas. Máximo anual de dedicación de 12 hombres mes (1575 horas)
Máximo anual para PDI de la Universidad Carlos III de Madrid de 8,8 hombres mes (1.155 horas)

EQUIPOS

Descripción	Coste (Euro)	% Uso dedicado proyecto	Dedicación (meses)	Período de depreciación	Coste imputable [d]
Pórtatil de trabajo	450,00	100	9	60	67,50
Microsoft Office 2007 Professional	290,00	10	1	60	0,48
Microsoft Office Project 2007	120,00	5	0,2	60	0,02
					0,00
				Total	68,00

[d] Fórmula de cálculo de la Amortización:

$$\frac{A}{B} x C x D$$

A = nº de meses desde la fecha de facturación en que el equipo es utilizado
B = período de depreciación (60 meses)
C = coste del equipo (sin IVA)
D = % del uso que se dedica al proyecto (habitualmente 100%)

SUBCONTRATACIÓN DE TAREAS

Descripción	Empresa	Coste imputable
	Total	0,00

OTROS COSTES DIRECTOS DEL PROYECTO[e]

Descripción	Empresa	Costes imputable
	Total	0,00

[e] Este capítulo de gastos incluye todos los gastos no contemplados en los conceptos anteriores, por ejemplo: fungible, viajes y dietas, otros,...

6.- Resumen de costes

Presupuesto Costes Totales	Presupuesto Costes Totales
Personal	1.181
Amortización	68
Subcontratación de tareas	0
Costes de funcionamiento	0
Costes Indirectos	250
Total	1.499

Figura 33. Presupuesto

CAPÍTULO 9

CONCLUSIONES

9. CONCLUSIONES

Actualmente, las compañías tienen la necesidad de conseguir mantener una imagen fiel de sus cuentas de cara a sus inversores. Para conseguir esto y dado que es conocido por todos la necesidad de controlar los sistemas donde se gestiona la información contable, es necesario cumplir las buenas prácticas en cuanto a tecnología se refiere así como contar con unas políticas que gobiernen en el área de sistemas de la compañía.

Dada la evolución de los sistemas de información y la mayor implicación de estos en los estados financieros de las compañías, así como el fuerte dimensionamiento e inversión que se está haciendo en los departamentos de auditoría interna de éstas, consideré como objetivo el crear un marco de evaluación que les permita a las compañías tener la posibilidad de evaluar el nivel de sus sistemas de información y la necesidad de desarrollar una aplicación sencilla que, con unos criterios mínimos, las compañías que deseen conocer sus mayores focos de debilidad en cuanto a sistemas se refiere, puedan identificar las mismas y establecerse planes de acción que ayuden a mitigar las mismas.

Un gran número de compañías tienen su información financiera tratada en los sistemas de información, siendo de mayor importancia que estos se encuentren controlados de forma adecuada.

La auditoría de controles generales de los sistemas de información es la revisión y evaluación de los controles que existen en los distintos sistemas, que nos aporta una perspectiva clave para enfocar una auditoría de cuentas. Dado que, en función del nivel de confianza que se deposite en los sistemas de donde la información se está extrayendo y, posteriormente es analizada por el equipo financiero, afectará en el volumen de trabajo realizado por este último en la correspondiente auditoría.

Es necesario, y con los resultados que he obtenido tras la realización de este Proyecto de Fin de Carrera, que las compañías evalúen la confianza en sus sistemas con el fin de poder garantizar una imagen fiel de la información que se genera desde los mismos y que, posteriormente, es analizada.

Como base de este proyecto, se ha analizado la Auditoría y el Control mediante la Sección 404 de la Ley Sarbanes-Oxley Act y, con dichos estudios se ha llevado a cabo un marco de metodología de cara a evaluar los Controles Generales de los Sistemas de la Información, implementándose de forma complementaria una aplicación que ayuda a la evaluación de la misma en la compañía.

Con la realización de este Proyecto de Fin de Carrera considero que he adquirido un mayor conocimiento del mundo de la auditoría, tanto desde el punto de vista de la importancia de realizar las mismas como de los distintos aspectos que se pueden analizar en ellas, y de los riesgos que pueden existir y materializarse debido a no contar con unos sistemas de información razonablemente controlados.

CAPÍTULO 10

LÍNEAS DE INVESTIGACIÓN FUTURAS

10. LÍNEAS DE INVESTIGACIÓN FUTURAS

Una vez llevado este trabajo de evaluación y desarrollo, crece la posibilidad de mejorar el estudio inicial realizado en este Proyecto de Fin de Carrera. Focalizándome en el estudio contemplado en este Proyecto surge la posibilidad de ampliar dicha aplicación desarrollada.

Esta aplicación podría ampliarse además de los controles generales de los sistemas de información, a los distintos procesos de negocio de las compañías y la evaluación de posibles controles automáticos definidos en los sistemas, de forma que una vez evaluado dichos controles generales, y siempre en cuando se obtenga una evaluación positiva se pueda establecer un marco de evaluación de los controles automáticos de dichos sistemas, como pudieran ser segregación de funciones, bloqueos, imposibilidad de modificaciones de datos, cálculos automáticos, etc.

Además, dicho desarrollo podría ser objeto de mejora desde los siguientes puntos de vista:

- Establecer una programación Web sustituyendo la aplicación para escritorio desarrollada, de forma que exista mayor facilidad para su instalación y uso, es decir, convertir la misma en un sistema más "friendly" para el usuario.
- Desde el punto de vista de la información analizada. Con esto quiero decir, que una vez que las evidencias fuesen analizadas, pudiesen adjuntarse a un repositorio integrado en la aplicación de forma que se pueda llevar a cabo un seguimiento, principalmente, de las debilidades encontradas en la revisión.
- Establecer una seguridad en el acceso a dicha aplicación, de forma que se encuentre controlado el acceso a las personas responsables de la auditoría.

Dado que, tanto las leyes como las Tecnologías de Información se encuentran en constante cambio, habría que considerar la posibilidad de realizar ciertas actualizaciones. Esto podría llevarse a cabo con un desarrollo en la nube, de forma que cualquier compañía indistintamente de donde se encuentre ubicada geográficamente pueda disponer de la posibilidad de utilizar la misma.

De este modo se ofrecería a las compañías un producto para optimizar sus costes y recursos, de forma que tengan una buena capacidad organizativa de las revisiones de los sistemas de información así como facilitar el seguimiento de dichos trabajos, por lo que sería un producto muy beneficioso para estudio futuro.

CAPÍTULO 11

ANEXO

11. ANEXO

11.1 GLOSARIO DE TÉRMINOS Y ACRÓNIMOS

A:

- Advisor: Consultor
- AI: Auditoría Interna
- APO: Administrar, Planear y Organizar

B:

- BAI: Build, Adquire and Implement
- Balanced Scoreboard: Cuadre de mando

C:

- CCO: Chief Communication Officer
- CEO: Chief Executive Officer
- CFO: Chief Financial Officer
- CGEIT: Certified in the Governance of Enterprise IT
- CIO: Chief Information Officer
- CII: Control Interno Informático
- CISA: Certified Information Systems Auditor
- CISM: Certified Information Security Manager
- CISO: Chief Information Security Officer
- COBIT: Control Objectives for Information Systems and related Technology
- Core: núcleo
- COSO: Committee of Sponsoring Organizations of the Treadway Commission
- CPD: Centro de Proceso de Datos
- CRISC: Certified in Risk and Information Systems Control
- CRO: Chief Running Officer

D:

- DS: Deliver and Support

E:

- EDM: Evaluar, Dirigir & Monitorear
- EDP: Electronic Data Process
- ERP: Enterprise Resource Planning

I:

- ICFR: Control Interno sobre Reporte Financiero
- IEC: International Electrotechnical Commission

- ISACA: Information Systems Audit and Control Association
- ISO: International Organization for Standardization
- IT: Information Technology
- ITGC: Information Technology General Control
- ITGI: Information Technology Govern Institute

M:

- Management: Dirección
- ME: Monitor and Evaluate

N:

- NASDAQ: National Association of Securities Dealers by Automatic Quotation
- NYSE: New York Stock Exchange

P:

- PCAOB: Public Company Accounting Oversight Board

R:

- RRHH: Recursos Humanos

S:

- SEC: Securities and Exchange Commission
- SI: Sistemas de la Información
- SOA: Sarbanes-Oxley Act
- SOX: Sarbanes-Oxley

T:

- TI: Tecnologías de la información

11.2 BIBLIOGRAFÍA

[1] La informatización en el proceso de Auditoría

http://www.monografias.com/

[2] Wikipedia

http://es.wikipedia.org/

[3] Control Interno y Auditoría Informática

http://myslide.es

[4] Generalidades en la auditoría

http://www.eumed.net/cursecon/libreria/rgl-genaud/indice.htm

[5] Auditoría externa, el análisis más objetivo

http://www.gestionyadministracion.com/auditoria/auditoria-externa.html

[6] Organismos de referencia

http://www.isaca.org/About-ISACA/History/Espanol/Pages/default.aspx

[7] Ley Sarbanes-Oxley

https://www.scribd.com/doc/54250844/Ley-Sarbanes-Oxley-Final

[8] Sarbanes-Oxley SOX

http://docplayer.es/4297499-Sarbanes-oxley-sox-agenda.html

[9] COSO, SOX, MEJORES PRACTICAS INTERNACIONALES EN CONTROL INTERNO

https://auditoriauc20102miju02.wikispaces.com/

[10] UAS 6 IT Control Objectives for SoX 3rd

http://blogs.itb.ac.id/el5007s1t2014d201523213151djokowintolo/cybersecurity/uas-6-it-control-objectives-for-sox-3rd/